Tenable.io Report

Tenable.io Report

Thu, 02 Jul 2020 11:37:10 UTC

Table Of Contents

Vulnerabilities By Host..... 3

- vda-it-ts..... 4

Vulnerabilities By Host

vda-it-ts

Scan Information

Start time:	2020/06/29 13:01
End time:	2020/06/29 15:12

Host Information

DNS Name:	vda-it-ts
Netbios Name:	VDA-IT-TS
OS:	[0: Microsoft Windows 10 Enterprise]

Results Summary

Critical	High	Medium	Low	Info	Total
1	2	10	1	128	142

Results Details

/

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2008/09/16, Modification date: 2020/06/23

Ports

vda-it-ts (UDP/4500) Vulnerability State: Active

```
Port 4500/udp was found to be open
```

vda-it-ts (TCP/49695) Vulnerability State: Active

```
Port 49695/tcp was found to be open
```

vda-it-ts (TCP/2105) Vulnerability State: Active

```
Port 2105/tcp was found to be open
```

vda-it-ts (TCP/49669) Vulnerability State: Active

```
Port 49669/tcp was found to be open
```

vda-it-ts (TCP/49698) Vulnerability State: Active

```
Port 49698/tcp was found to be open
```

vda-it-ts (UDP/56412) Vulnerability State: Active

```
Port 56412/udp was found to be open
```

vda-it-ts (UDP/65049) Vulnerability State: Active

```
Port 65049/udp was found to be open
```

vda-it-ts (UDP/62020) Vulnerability State: Active

```
Port 62020/udp was found to be open
```

vda-it-ts (UDP/54069) Vulnerability State: Active

```
Port 54069/udp was found to be open
```

vda-it-ts (UDP/123) Vulnerability State: Active

```
Port 123/udp was found to be open
```

vda-it-ts (UDP/5355) Vulnerability State: Active

```
Port 5355/udp was found to be open
```

vda-it-ts (UDP/54032) Vulnerability State: Active

```
Port 54032/udp was found to be open
```

vda-it-ts (UDP/161) Vulnerability State: Active

```
Port 161/udp was found to be open
```

vda-it-ts (UDP/56893) Vulnerability State: Active

```
Port 56893/udp was found to be open
```

vda-it-ts (UDP/63742) Vulnerability State: Active

```
Port 63742/udp was found to be open
```

vda-it-ts (TCP/0) Vulnerability State: Active

```

Nessus was able to find 66 open ports.
```

vda-it-ts (UDP/54827) Vulnerability State: Active

```
Port 54827/udp was found to be open
```

vda-it-ts (TCP/49671) Vulnerability State: Active

```
Port 49671/tcp was found to be open
```

vda-it-ts (UDP/53068) Vulnerability State: Active

```
Port 53068/udp was found to be open
```

vda-it-ts (UDP/55650) Vulnerability State: Active

```
Port 55650/udp was found to be open
```

vda-it-ts (UDP/50784) Vulnerability State: Active

```
Port 50784/udp was found to be open
```

vda-it-ts (TCP/3389) Vulnerability State: Active

```
Port 3389/tcp was found to be open
```

vda-it-ts (UDP/61075) Vulnerability State: Active

```
Port 61075/udp was found to be open
```

vda-it-ts (UDP/49318) Vulnerability State: Active

```
Port 49318/udp was found to be open
```

vda-it-ts (UDP/55383) Vulnerability State: Active

```
Port 55383/udp was found to be open
```

vda-it-ts (UDP/57075) Vulnerability State: Active

```
Port 57075/udp was found to be open
```

vda-it-ts (TCP/49666) Vulnerability State: Active

```
Port 49666/tcp was found to be open
```

vda-it-ts (UDP/57950) Vulnerability State: Active

```
Port 57950/udp was found to be open
```

vda-it-ts (TCP/2107) Vulnerability State: Active

```
Port 2107/tcp was found to be open
```

vda-it-ts (UDP/53729) Vulnerability State: Active

```
Port 53729/udp was found to be open
```

vda-it-ts (TCP/49664) Vulnerability State: Active

Port 49664/tcp was found to be open

vda-it-ts (UDP/49981) Vulnerability State: Active

Port 49981/udp was found to be open

vda-it-ts (UDP/53069) Vulnerability State: Active

Port 53069/udp was found to be open

vda-it-ts (UDP/63118) Vulnerability State: Active

Port 63118/udp was found to be open

vda-it-ts (UDP/51502) Vulnerability State: Active

Port 51502/udp was found to be open

vda-it-ts (TCP/49704) Vulnerability State: Active

Port 49704/tcp was found to be open

vda-it-ts (UDP/5050) Vulnerability State: Active

Port 5050/udp was found to be open

vda-it-ts (TCP/5040) Vulnerability State: Active

Port 5040/tcp was found to be open

vda-it-ts (TCP/1801) Vulnerability State: Active

Port 1801/tcp was found to be open

vda-it-ts (UDP/3389) Vulnerability State: Active

Port 3389/udp was found to be open

vda-it-ts (UDP/63929) Vulnerability State: Active

Port 63929/udp was found to be open

vda-it-ts (UDP/51493) Vulnerability State: Active

Port 51493/udp was found to be open

vda-it-ts (UDP/3249) Vulnerability State: Active

Port 3249/udp was found to be open

vda-it-ts (UDP/54070) Vulnerability State: Active

Port 54070/udp was found to be open

vda-it-ts (UDP/1900) Vulnerability State: Active

Port 1900/udp was found to be open

vda-it-ts (TCP/49670) Vulnerability State: Active

Port 49670/tcp was found to be open

vda-it-ts (UDP/55391) Vulnerability State: Active

Port 55391/udp was found to be open

vda-it-ts (UDP/65328) Vulnerability State: Active

Port 65328/udp was found to be open

vda-it-ts (UDP/60323) Vulnerability State: Active

Port 60323/udp was found to be open

vda-it-ts (UDP/500) Vulnerability State: Active

Port 500/udp was found to be open

vda-it-ts (TCP/55507) Vulnerability State: Active

Port 55507/tcp was found to be open

vda-it-ts (UDP/62034) Vulnerability State: Active

Port 62034/udp was found to be open

vda-it-ts (UDP/5353) Vulnerability State: Active

Port 5353/udp was found to be open

vda-it-ts (TCP/49665) Vulnerability State: Active

```
Port 49665/tcp was found to be open
```

vda-it-ts (TCP/49700) Vulnerability State: Active

```
Port 49700/tcp was found to be open
```

vda-it-ts (TCP/49685) Vulnerability State: Active

```
Port 49685/tcp was found to be open
```

vda-it-ts (TCP/60168) Vulnerability State: Active

```
Port 60168/tcp was found to be open
```

vda-it-ts (UDP/55091) Vulnerability State: Active

```
Port 55091/udp was found to be open
```

vda-it-ts (TCP/135) Vulnerability State: Active

```
Port 135/tcp was found to be open
```

vda-it-ts (UDP/54775) Vulnerability State: Active

```
Port 54775/udp was found to be open
```

vda-it-ts (UDP/55395) Vulnerability State: Active

```
Port 55395/udp was found to be open
```

vda-it-ts (TCP/445) Vulnerability State: Active

```
Port 445/tcp was found to be open
```

vda-it-ts (UDP/64772) Vulnerability State: Active

```
Port 64772/udp was found to be open
```

vda-it-ts (UDP/54776) Vulnerability State: Active

```
Port 54776/udp was found to be open
```

vda-it-ts (TCP/2103) Vulnerability State: Active

```
Port 2103/tcp was found to be open
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2008/09/23, Modification date: 2020/06/23

Ports

vda-it-ts (UDP/54776) Vulnerability State: New

```
The Win32 process 'spoolsv.exe' is listening on this port (pid 3688).

This process 'spoolsv.exe' (pid 3688) is hosting the following Windows services :
Spooler (@%systemroot%\system32\spoolsv.exe,-1)
```

vda-it-ts (TCP/49671) Vulnerability State: New

```
The Win32 process 'lsass.exe' is listening on this port (pid 748).

This process 'lsass.exe' (pid 748) is hosting the following Windows services :
EFS (@%SystemRoot%\system32\efssvc.dll,-100)
KeyIso (@keyiso.dll,-100)
Netlogon (@%SystemRoot%\System32\netlogon.dll,-102)
```

```
SamSs (@%SystemRoot%\system32\samsrv.dll,-1)
VaultSvc (@%SystemRoot%\system32\vaultsvc.dll,-1003)
```

vda-it-ts (TCP/3389) Vulnerability State: New

```
The Win32 process 'svchost.exe' is listening on this port (pid 1032).

This process 'svchost.exe' (pid 1032) is hosting the following Windows services :
TermService (@%SystemRoot%\System32\termsrv.dll,-268)
```

vda-it-ts (UDP/62034) Vulnerability State: New

```
The Win32 process 'EXCEL.EXE' is listening on this port (pid 174492).
```

vda-it-ts (TCP/49669) Vulnerability State: New

```
The Win32 process 'svchost.exe' is listening on this port (pid 2488).

This process 'svchost.exe' (pid 2488) is hosting the following Windows services :
Schedule (@%SystemRoot%\system32\schedsvc.dll,-100)
```

vda-it-ts (UDP/55391) Vulnerability State: New

```
The Win32 process 'Fuze.exe' is listening on this port (pid 12776).
```

vda-it-ts (UDP/1900) Vulnerability State: New

```
The Win32 process 'svchost.exe' is listening on this port (pid 6844).

This process 'svchost.exe' (pid 6844) is hosting the following Windows services :
SSDPSRV (@%systemroot%\system32\ssdpsrv.dll,-100)
```

vda-it-ts (UDP/53729) Vulnerability State: New

```
The Win32 process 'svchost.exe' is listening on this port (pid 2040).

This process 'svchost.exe' (pid 2040) is hosting the following Windows services :
LanmanWorkstation (@%systemroot%\system32\wkssvc.dll,-100)
```

vda-it-ts (UDP/54070) Vulnerability State: New

```
The Win32 process 'SavService.exe' is listening on this port (pid 3300).

This process 'SavService.exe' (pid 3300) is hosting the following Windows services :
SAVService (Sophos Anti-Virus)
```

vda-it-ts (UDP/57950) Vulnerability State: New

```
The Win32 process 'OUTLOOK.EXE' is listening on this port (pid 352992).
```

vda-it-ts (UDP/55395) Vulnerability State: New

```
The Win32 process 'Fuze.exe' is listening on this port (pid 12776).
```

vda-it-ts (TCP/49664) Vulnerability State: New

```
The Win32 process 'lsass.exe' is listening on this port (pid 748).

This process 'lsass.exe' (pid 748) is hosting the following Windows services :
EFS (@%SystemRoot%\system32\efssvc.dll,-100)
KeyIso (@keyiso.dll,-100)
Netlogon (@%SystemRoot%\System32\netlogon.dll,-102)
SamSs (@%SystemRoot%\system32\samsrv.dll,-1)
VaultSvc (@%SystemRoot%\system32\vaultsvc.dll,-1003)
```

vda-it-ts (TCP/1801) Vulnerability State: New

```
The Win32 process 'mqsvc.exe' is listening on this port (pid 4248).

This process 'mqsvc.exe' (pid 4248) is hosting the following Windows services :
MSMQ (@mqutil.dll,-6102)
```

vda-it-ts (UDP/57075) Vulnerability State: New

```
The Win32 process 'svchost.exe' is listening on this port (pid 2280).

This process 'svchost.exe' (pid 2280) is hosting the following Windows services :
NlaSvc (@%SystemRoot%\System32\nlasvc.dll,-1)
```

vda-it-ts (TCP/445) Vulnerability State: New

```
The Win32 process 'System' is listening on this port (pid 4).
```

vda-it-ts (TCP/5040) Vulnerability State: New

```
The Win32 process 'svchost.exe' is listening on this port (pid 3584).

This process 'svchost.exe' (pid 3584) is hosting the following Windows services :
CDPSvc (@%SystemRoot%\system32\cdpsvc.dll,-100)
```

vda-it-ts (UDP/161) Vulnerability State: New

```
The Win32 process 'snmp.exe' is listening on this port (pid 4160).

This process 'snmp.exe' (pid 4160) is hosting the following Windows services :
SNMP (@firewallapi.dll,-50303)
```

vda-it-ts (TCP/60168) Vulnerability State: New

```
The Win32 process 'unsecapp.exe' is listening on this port (pid 11556).
```

vda-it-ts (TCP/2103) Vulnerability State: New

```
The Win32 process 'mqsvc.exe' is listening on this port (pid 4248).

This process 'mqsvc.exe' (pid 4248) is hosting the following Windows services :
MSMQ (@mqutil.dll,-6102)
```

vda-it-ts (UDP/4500) Vulnerability State: New

```
The Win32 process 'svchost.exe' is listening on this port (pid 1588).

This process 'svchost.exe' (pid 1588) is hosting the following Windows services :
IKEEXT (@%SystemRoot%\system32\ikeext.dll,-501)
```

vda-it-ts (UDP/63929) Vulnerability State: New

```
The Win32 process 'svchost.exe' is listening on this port (pid 6844).

This process 'svchost.exe' (pid 6844) is hosting the following Windows services :
SSDPSRV (@%systemroot%\system32\ssdpsrv.dll,-100)
```

vda-it-ts (UDP/56893) Vulnerability State: New

```
The Win32 process 'svchost.exe' is listening on this port (pid 1768).

This process 'svchost.exe' (pid 1768) is hosting the following Windows services :
iphlpsvc (@%SystemRoot%\system32\iphlpsvc.dll,-500)
```

vda-it-ts (UDP/65328) Vulnerability State: New

```
The Win32 process 'SavService.exe' is listening on this port (pid 3300).

This process 'SavService.exe' (pid 3300) is hosting the following Windows services :
SAVService (Sophos Anti-Virus)
```

vda-it-ts (UDP/54775) Vulnerability State: New

```
The Win32 process 'SavService.exe' is listening on this port (pid 3300).

This process 'SavService.exe' (pid 3300) is hosting the following Windows services :
SAVService (Sophos Anti-Virus)
```

vda-it-ts (TCP/49695) Vulnerability State: New

```
The Win32 process 'svchost.exe' is listening on this port (pid 1660).

This process 'svchost.exe' (pid 1660) is hosting the following Windows services :
PolicyAgent (@%SystemRoot%\System32\polstore.dll,-5010)
```

vda-it-ts (TCP/49685) Vulnerability State: New

```
The Win32 process 'svchost.exe' is listening on this port (pid 3172).

This process 'svchost.exe' (pid 3172) is hosting the following Windows services :
SessionEnv (@%SystemRoot%\System32\SessEnv.dll,-1026)
```

vda-it-ts (UDP/63742) Vulnerability State: New

```
The Win32 process 'WmiPrvSE.exe' is listening on this port (pid 4668).
```

vda-it-ts (TCP/135) Vulnerability State: New

```
The Win32 process 'svchost.exe' is listening on this port (pid 448).

This process 'svchost.exe' (pid 448) is hosting the following Windows services :
RpcEptMapper (@%windir%\system32\RpcEpMap.dll,-1001)
RpcSs (@combase.dll,-5010)
```

vda-it-ts (TCP/49670) Vulnerability State: New

```
The Win32 process 'spoolsv.exe' is listening on this port (pid 3688).

This process 'spoolsv.exe' (pid 3688) is hosting the following Windows services :
Spooler (@%systemroot%\system32\spoolsv.exe,-1)
```

vda-it-ts (UDP/63118) Vulnerability State: New

```
The Win32 process 'Fuze.exe' is listening on this port (pid 12776).
```

vda-it-ts (UDP/53068) Vulnerability State: New

```
The Win32 process 'swi_service.exe' is listening on this port (pid 4500).

This process 'swi_service.exe' (pid 4500) is hosting the following Windows services :
swi_service (Sophos Web Intelligence Service)
```

vda-it-ts (UDP/5353) Vulnerability State: New

```
The Win32 process 'chrome.exe' is listening on this port (pid 345536).
```

vda-it-ts (TCP/49700) Vulnerability State: New

```
The Win32 process 'swi_fc.exe' is listening on this port (pid 5848).
```

vda-it-ts (UDP/55650) Vulnerability State: New

```
The Win32 process 'SavService.exe' is listening on this port (pid 3300).

This process 'SavService.exe' (pid 3300) is hosting the following Windows services :
SAVService (Sophos Anti-Virus)
```

vda-it-ts (UDP/500) Vulnerability State: New

```
The Win32 process 'svchost.exe' is listening on this port (pid 1588).

This process 'svchost.exe' (pid 1588) is hosting the following Windows services :
IKEEXT (@%SystemRoot%\system32\ikeext.dll,-501)
```

vda-it-ts (UDP/56412) Vulnerability State: New

```
The Win32 process 'lsass.exe' is listening on this port (pid 748).

This process 'lsass.exe' (pid 748) is hosting the following Windows services :
EFS (@%SystemRoot%\system32\efssvc.dll,-100)
KeyIso (@keyiso.dll,-100)
Netlogon (@%SystemRoot%\System32\netlogon.dll,-102)
SamSs (@%SystemRoot%\system32\samsrv.dll,-1)
VaultSvc (@%SystemRoot%\system32\vaultsvc.dll,-1003)
```

vda-it-ts (TCP/49666) Vulnerability State: New

```
The Win32 process 'svchost.exe' is listening on this port (pid 2000).

This process 'svchost.exe' (pid 2000) is hosting the following Windows services :
EventLog (@%SystemRoot%\system32\wevtsvc.dll,-200)
```

vda-it-ts (UDP/54032) Vulnerability State: New

```
The Win32 process 'SavService.exe' is listening on this port (pid 3300).

This process 'SavService.exe' (pid 3300) is hosting the following Windows services :
SAVService (Sophos Anti-Virus)
```

vda-it-ts (UDP/62020) Vulnerability State: New

```
The Win32 process 'SavService.exe' is listening on this port (pid 3300).

This process 'SavService.exe' (pid 3300) is hosting the following Windows services :
SAVService (Sophos Anti-Virus)
```

vda-it-ts (UDP/49981) Vulnerability State: New

```
The Win32 process 'POWERPNT.EXE' is listening on this port (pid 56052).
```

vda-it-ts (UDP/54069) Vulnerability State: New

```
The Win32 process 'SavService.exe' is listening on this port (pid 3300).

This process 'SavService.exe' (pid 3300) is hosting the following Windows services :
SAVService (Sophos Anti-Virus)
```

vda-it-ts (UDP/53069) Vulnerability State: New

```
The Win32 process 'swi_service.exe' is listening on this port (pid 4500).

This process 'swi_service.exe' (pid 4500) is hosting the following Windows services :
swi_service (Sophos Web Intelligence Service)
```

vda-it-ts (TCP/55507) Vulnerability State: New

```
The Win32 process 'svchost.exe' is listening on this port (pid 1604).

This process 'svchost.exe' (pid 1604) is hosting the following Windows services :
Winmgmt (@%Systemroot%\system32\wbem\wmisvc.dll,-205)
```

vda-it-ts (TCP/49704) Vulnerability State: New

```
The Win32 process 'services.exe' is listening on this port (pid 712).
```

vda-it-ts (TCP/49665) Vulnerability State: New

```
The Win32 process 'wininit.exe' is listening on this port (pid 588).
```

vda-it-ts (UDP/3389) Vulnerability State: New

```
The Win32 process 'svchost.exe' is listening on this port (pid 1032).

This process 'svchost.exe' (pid 1032) is hosting the following Windows services :
TermService (@%SystemRoot%\System32\termsrv.dll,-268)
```

vda-it-ts (TCP/2107) Vulnerability State: New

```
The Win32 process 'mqsvc.exe' is listening on this port (pid 4248).

This process 'mqsvc.exe' (pid 4248) is hosting the following Windows services :
MSMQ (@mqutil.dll,-6102)
```

vda-it-ts (UDP/50784) Vulnerability State: New

```
The Win32 process 'OUTLOOK.EXE' is listening on this port (pid 352992).
```

vda-it-ts (UDP/55091) Vulnerability State: New

```
The Win32 process 'SavService.exe' is listening on this port (pid 3300).

This process 'SavService.exe' (pid 3300) is hosting the following Windows services :
SAVService (Sophos Anti-Virus)
```

vda-it-ts (UDP/3249) Vulnerability State: New

```
The Win32 process 'msddsk.exe' is listening on this port (pid 11496).
```

vda-it-ts (UDP/49318) Vulnerability State: New

```
The Win32 process 'SavService.exe' is listening on this port (pid 3300).

This process 'SavService.exe' (pid 3300) is hosting the following Windows services :
SAVService (Sophos Anti-Virus)
```

vda-it-ts (UDP/51493) Vulnerability State: New

```
The Win32 process 'Teams.exe' is listening on this port (pid 14452).
```

vda-it-ts (TCP/2105) Vulnerability State: New

```
The Win32 process 'mqsvc.exe' is listening on this port (pid 4248).

This process 'mqsvc.exe' (pid 4248) is hosting the following Windows services :
MSMQ (@mqutil.dll,-6102)
```

vda-it-ts (UDP/64772) Vulnerability State: New

```
The Win32 process 'SavService.exe' is listening on this port (pid 3300).

This process 'SavService.exe' (pid 3300) is hosting the following Windows services :
```

```
SAVService (Sophos Anti-Virus)
```

vda-it-ts (UDP/5050) Vulnerability State: New

```
The Win32 process 'svchost.exe' is listening on this port (pid 3584).

This process 'svchost.exe' (pid 3584) is hosting the following Windows services :
CDPSvc (@%SystemRoot%\system32\cdpsvc.dll,-100)
```

vda-it-ts (UDP/123) Vulnerability State: New

```
The Win32 process 'svchost.exe' is listening on this port (pid 1064).

This process 'svchost.exe' (pid 1064) is hosting the following Windows services :
W32Time (@%SystemRoot%\system32\w32time.dll,-200)
```

vda-it-ts (UDP/65049) Vulnerability State: New

```
The Win32 process 'SavService.exe' is listening on this port (pid 3300).

This process 'SavService.exe' (pid 3300) is hosting the following Windows services :
SAVService (Sophos Anti-Virus)
```

vda-it-ts (UDP/5355) Vulnerability State: New

```
The Win32 process 'svchost.exe' is listening on this port (pid 1204).

This process 'svchost.exe' (pid 1204) is hosting the following Windows services :
Dnscache (@%SystemRoot%\System32\dnsapi.dll,-101)
```

vda-it-ts (TCP/49698) Vulnerability State: New

```
The Win32 process 'mqsvc.exe' is listening on this port (pid 4248).

This process 'mqsvc.exe' (pid 4248) is hosting the following Windows services :
MSMQ (@mqutil.dll,-6102)
```

vda-it-ts (UDP/60323) Vulnerability State: New

```
The Win32 process 'SavService.exe' is listening on this port (pid 3300).

This process 'SavService.exe' (pid 3300) is hosting the following Windows services :
SAVService (Sophos Anti-Virus)
```

vda-it-ts (UDP/55383) Vulnerability State: New

```
The Win32 process 'Fuze.exe' is listening on this port (pid 12776).
```

vda-it-ts (UDP/61075) Vulnerability State: New

```
The Win32 process 'WINWORD.EXE' is listening on this port (pid 359440).
```

vda-it-ts (UDP/54827) Vulnerability State: New

```
The Win32 process 'SavService.exe' is listening on this port (pid 3300).

This process 'SavService.exe' (pid 3300) is hosting the following Windows services :
SAVService (Sophos Anti-Virus)
```

vda-it-ts (UDP/51502) Vulnerability State: New

```
The Win32 process 'MAT.UI.exe' is listening on this port (pid 354320).
```

100574 - Tenable Windows Nessus Agent Installed

Synopsis

A vulnerability scanning application is installed on the remote Windows host.

Description

Tenable Windows Nessus Agent, an agent for the Tenable Nessus vulnerability scanner, is installed on the remote Windows host.

See Also

https://www.tenable.com/products/nessus/nessus-agents

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2017/06/01, Modification date: 2020/06/23

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Path    : C:\Program Files\Tenable\Nessus Agent
Version : 7.7.0.20021
```

92413 - 7-Zip Recent Files

Synopsis

Nessus was able to enumerate recently accessed 7-Zip compressed files on the remote host.

Description

Nessus was able to query 7-Zip settings on the remote Windows host to find recently accessed compressed files.

See Also

https://www.7-zip.org/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2018/11/15

Ports

vda-it-ts (TCP/0) Vulnerability State: Resurfaced

```
EDENBROWN.UK\t.styles
 - C:\temp\bi\Ops_Dashboard v3.pbix\Report\
 - C:\temp\bi\Ops_Dashboard v3.pbix\
 - C:\temp\PBI\Ops_Dashboard v3.pbix\Report\
 - C:\temp\PBI\Ops_Dashboard v3.pbix\
 - C:\temp\PBI\Ops_Dashboard v3.pbix\Report\CustomVisuals\
```

92429 - Recycle Bin Files

Synopsis

Nessus was able to enumerate files in the recycle bin on the remote host.

Description

Nessus was able to generate a list of all files found in $Recycle.Bin subdirectories.

See Also

http://www.nessus.org/u?0c1a03df

http://www.nessus.org/u?61293b38

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2018/11/15

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
[...]
```

92421 - Internet Explorer Typed URLs

Synopsis

Nessus was able to enumerate URLs that were manually typed into the Internet Explorer address bar.

Description

Nessus was able to generate a list URLs that were manually typed into the Internet Explorer address bar.

See Also

https://crucialsecurityblog.harris.com/2011/03/14/typedurls-part-1/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2018/05/16

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
 https://uk.comensura.net/v4/Handler.aspx
https://meetme.i-resource.co.uk/
http://localhost/login.aspx?ReturnUrl=%2fMsp%2fDashboard.aspx
http://sql02/Reports/Pages/Report.aspx?ItemPath=%2fFinancial_Reports%2fPO+number
+change&ViewMode=Detail
http://www.synergymedicalhealth.co.uk/
http://sql03/reports
http://localhost/ReportServer/pages/report.aspx?bi_reports/
Consultant_Dashboard&rs:Format=EXCEL&rs:Command=Render&EmployerRef=CAR001&ConsultantCode=PAChttp://
localhost/ReportServer/pages/report.aspx?bi_reports/
Consultant_Dashboard&rs:Format=EXCEL&rs:Command=Render&EmployerRef=CAR001&ConsultantCode=PAChttp://
localhost/ReportServer/pages/report.aspx?bi_reports/
Consultant_Dashboard&rs:Format=EXCEL&rs:Command=Render&EmployerRef=CAR001&ConsultantCode=PAC
http://sql02/Reports/Pages/Folder.aspx?ItemPath=%2fssrs_reports
https://app.powerbi.com/reportEmbed?reportId=59bb27e4-
ddba-4059-8d24-403f7e753521&autoAuth=true&ctid=1726bc0b-9288-4c47-a2ee-
cb4eace528d9&config=eyJjbHVzdGVyVXJsIjoiaHR0cHM6Ly93YWJpLW5vcnRoLWV1cm9wZS1yZWRpcmVjdC5hbmFseXNpcy53aW5kb3dzLm
%3D%3D
http://sql02/ReportServer/pages/report.aspx?bi_reports/
Consultant_Dashboard&rs:Format=EXCEL&rs:Command=Render&EmployerRef=CAR001&ConsultantCode=PAC
https://app.powerbi.com/
http://www.bbc.co.uk/
https://www.google.co.uk/
http://bi01/Reports/Pages/Report.aspx?ItemPath=%2fVMS365_DW_Reports%2fNHSI_Report
http://sql-lab/ebs-jobs/
http://sql02/Reports/Pages/Report.aspx?ItemPath=%2fssrs_reports%2fNow+We+Comply+Report
microsoft.reportingservices.reportprocessing.reportprocessingexception: There is no data for the
 field at [...]
```

20862 - Mozilla Foundation Application Detection

Synopsis

The remote Windows host contains one or more applications from the Mozilla Foundation.

Description

There is at least one instance of Firefox, Thunderbird, SeaMonkey, or the Mozilla browser installed on the remote Windows host.

See Also

https://www.mozilla.org/en-US/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2006/02/05, Modification date: 2019/11/22

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Product : Mozilla Firefox
Path    : C:\Program Files (x86)\Mozilla Firefox
Version : 77.0.1

Product : Mozilla Firefox
Path    : C:\Program Files\Mozilla Firefox
Version : 77.0.1
```

92220 - Microsoft Visio Installed (credentialed check)

Synopsis

A diagramming application is installed on the remote host.

Description

Microsoft Visio, a diagramming and vector graphics application, is installed on the remote Windows host.

See Also

https://products.office.com/en-us/visio/flowchart-software

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/07/14, Modification date: 2020/06/12

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Path         : C:\Program Files\Microsoft Office\Office14\Visio.exe
Version      : 14.0.7248.5000
Product      : 2010
Service Pack : 2
```

17651 - Microsoft Windows SMB : Obtains the Password Policy

Synopsis

It is possible to retrieve the remote host's password policy using the supplied credentials.

Description

Using the supplied credentials it was possible to extract the password policy for the remote Windows host. The password policy must conform to the Informational System Policy.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/03/30, Modification date: 2015/01/12

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
The following password policy is defined on the remote host:

Minimum password len: 14
Password history len: 20
Maximum password age (d): 90
Password must meet complexity requirements: Enabled
Minimum password age (d): 0
Forced logoff time (s): Not set
Locked account time (s): 1800
Time between failed logon (s): 900
Number of invalid logon before locked out (s): 10
```

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

See Also

https://standards.ieee.org/faqs/regauth.html

http://www.nessus.org/u?794673b4

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/02/19, Modification date: 2020/05/13

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
The following card manufacturers were identified :

00:50:56:A6:49:57 : VMware, Inc.
```

122546 - Microsoft Visual Studio Isolated Shell Installed

Synopsis

The remote Windows host has one or more applications built on top of Microsoft Visual Studio Isolated Shell.

Description

Microsoft Visual Studio Isolated Shell, a base IDE to build tools and applications on top of Visual Studio, is installed on the remote Windows host.

See Also

https://visualstudio.microsoft.com/vs/older-downloads/isolated-shell/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2019/03/04, Modification date: 2020/06/23

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Path    : c:\Program Files (x86)\Microsoft Visual Studio 10.0\
Version : 10.0.40219.1
Product : 2010
```

92434 - User Download Folder Files

Synopsis

Nessus was able to enumerate downloaded files on the remote host.

Description

Nessus was able to generate a report of all files listed in the default user download folder.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2018/05/16

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
 C:\\Users\Administrator\Downloads\desktop.ini
C:\\Users\ITaccount\Downloads\desktop.ini
C:\\Users\Public\Downloads\desktop.ini
C:\\Users\t.styles\Downloads\00ebe936-2a1c-4348-88ab-75f3c6b64eef.CSV
C:\\Users\t.styles\Downloads\01 Jan.zip
C:\\Users\t.styles\Downloads\03 June 2019_RX Nursing & Synergy medical.xlsx
C:\\Users\t.styles\Downloads\039d63ec-ac0d-4c71-baf3-935a9f535ab9.jpg
C:\\Users\t.styles\Downloads\070356048604-20181221-1419.pdf
C:\\Users\t.styles\Downloads\070356048604-20181221-1425.csv
C:\\Users\t.styles\Downloads
\11422161_93ab47ca2c6c85216726ba1db49b4fa74061096a81465505de9805e2cfbc524d(1).pdf
C:\\Users\t.styles\Downloads
\11422161_93ab47ca2c6c85216726ba1db49b4fa74061096a81465505de9805e2cfbc524d.pdf
C:\\Users\t.styles\Downloads
\11422218_d17c72950e0fdb27db88a5806e5c140d4bbe87495796646add92a9169d7f35b8(1).pdf
C:\\Users\t.styles\Downloads
\11422218_d17c72950e0fdb27db88a5806e5c140d4bbe87495796646add92a9169d7f35b8.pdf
C:\\Users\t.styles\Downloads\132653_CLIENTPACK_V17.pdf
C:\\Users\t.styles\Downloads\132653_CLIENTPACK_V19.pdf
C:\\Users\t.styles\Downloads\132653_INVSYS_V23.pdf
C:\\Users\t.styles\Downloads\141A676BB7529B6915236AD474F12861.ics
C:\\Users\t.styles\Downloads\1530779312-92969-Debbie_Skeete_CV_July_2018 (1).zip
C:\\Users\t.styles\Downloads\1530779312-92969-Debbie_Skeete_CV_July_2018.zip
C:\\Users\t.styles\Downloads\1b225af6-3689-4a34-9111-76c2eef84e8e.CSV
C:\\Users\t.styles\Downloads\200719927.zip
C:\\Users\t.styles\Downloads\2014_Budget (in progress) (1).xlsx
C:\\Users\t.styles\Downloads\2014_Budget (in progress) (TS) (1).xlsx
C:\\Users\t.styles\Downloads\2014_Budget (in progress) (TS) (2).xlsx
C:\\Users\t.styles\Downloads\2014_Budget (in progress) (TS).xlsx
C:\\Users\t.styles\Downloads\2014_Budget (in progress).xlsx
C:\\Users\t.styles\Downloads\2017_PermData_20180702.xlsx
C:\\Users\t.styles\Downloads\20180702171152933.pdf
C:\\Users\t.styles\Downloads\20181010_Export_Count_of_Active_Devices_nGAGE Specialist Recruitment
 [...]
```

34196 - Google Chrome Detection (Windows)

Synopsis

The remote Windows host contains a web browser.

Description

Google Chrome, a web browser from Google, is installed on the remote Windows host.

See Also

https://www.google.com/chrome/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2008/09/12, Modification date: 2019/11/22

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Path    : C:\Program Files (x86)\Google\Chrome\Application
Version : 83.0.4103.116
```

126604 - Security Updates for Microsoft Visual Studio Products (July 2019)

Synopsis

The Microsoft Visual Studio Products are affected by multiple vulnerabilities.

Description

The Microsoft Visual Studio Products are missing security updates. It is, therefore, affected by multiple vulnerabilities:
- An information disclosure vulnerability exists when Visual Studio improperly parses XML input in certain settings files. An attacker who successfully exploited this vulnerability could read arbitrary files via an XML external entity (XXE) declaration. (CVE-2019-1079)
- A remote code execution vulnerability exists in .NET software when the software fails to check the source markup of a file. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. (CVE-2019-1113)
- An elevation of privilege vulnerability exists when the Visual Studio updater service improperly handles file permissions. An attacker who successfully exploited this vulnerability overwrite arbitrary files with XML content in the security context of the local system. (CVE-2019-1077)

See Also

http://www.nessus.org/u?0160558d

http://www.nessus.org/u?8979a8ff

http://www.nessus.org/u?9d195815

http://www.nessus.org/u?e0583a4c

http://www.nessus.org/u?04ba0c0e

http://www.nessus.org/u?d6fee2f9

http://www.nessus.org/u?fe31e5ea

http://www.nessus.org/u?e30ad270

Solution

Microsoft has released the following security updates to address this issue:
-KB4506161
-KB4506162
-KB4506163
-KB4506164

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

5.9

CVSS v3.0 Base Score

8.8 (AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.7 (E:U/RL:O/RC:C)

CVSS Base Score

6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

5.0 (E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2019-1077
CVE	CVE-2019-1113
CVE	CVE-2019-1079
BID	108977
BID	108931
XREF	MSFT:MS19-4506163
XREF	MSFT:MS19-4506164
XREF	MSFT:MS19-4506161
XREF	MSFT:MS19-4506162
XREF	IAVA:2019-A-0225
XREF	MSKB:4506161
XREF	MSKB:4506162
XREF	MSKB:4506163
XREF	MSKB:4506164

Plugin Information:

Publication date: 2019/07/11, Modification date: 2019/10/18

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Note: The fix for this issue is available in the following update:

  - KB4506163 : Security update for the information disclosure vulnerability in Microsoft Visual
 Studio 2013 Update 5: July 9, 2019
```

69475 - FileZilla Client Installed

Synopsis

An open source FTP client is installed on the remote host.

Description

FileZilla, an open source FTP/SFTP client, is installed on the remote host.

See Also

https://filezilla-project.org/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/08/13, Modification date: 2019/11/22

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Path    : C:\Program Files\FileZilla FTP Client\FileZilla.exe
Version : 3.48.1.0
```

45050 - WMI Anti-spyware Enumeration

Synopsis

It is possible to obtain the list of anti-spyware software installed on the remote Windows host.

Description

By connecting to the remote Windows host with the supplied credentials, this plugin uses WMI to enumerate anti-spyware software installed on it.
Note that this plugin extracts this information from the 'root\securitycenter' and 'root\securitycenter2' WMI namespaces, which are only available in Windows desktop operating systems such as XP, Vista and Windows 7.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/03/12, Modification date: 2020/06/23

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
Here is the list of anti-spyware software registered under the
'root\SecurityCenter2' WMI namespace :

+ Sophos Anti-Virus

  - pathToSignedProductExe : C:\Program Files (x86)\Sophos\Sophos Anti-Virus\WSCClient.exe
  - pathToSignedReportingExe : C:\Program Files (x86)\Sophos\Sophos Anti-Virus\WSCClient.exe
  - productState : 331776

+ Windows Defender

  - pathToSignedProductExe : windowsdefender://
  - pathToSignedReportingExe : %ProgramFiles%\Windows Defender\MsMpeng.exe
  - productState : 393472
```

92415 - Application Compatibility Cache

Synopsis

Nessus was able to gather application compatibility settings on the remote host.

Description

Nessus was able to generate a report on the application compatibility cache on the remote Windows host.

See Also

https://dl.mandiant.com/EE/library/Whitepaper_ShimCacheParser.pdf

http://www.nessus.org/u?4a076105

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2018/05/23

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
Application compatibility cache report attached.
```

62042 - SMB QuickFixEngineering (QFE) Enumeration

Synopsis

The remote host has quick-fix engineering updates installed.

Description

By connecting to the host with the supplied credentials, this plugin enumerates quick-fix engineering updates installed on the remote host via the registry.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2012/09/11, Modification date: 2020/06/12

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
Here is a list of quick-fix engineering updates installed on the
remote system :

KB4493478, Installed on: 2019/08/05
KB4497165, Installed on: 2020/06/02
KB4502496, Installed on: 2020/02/13
KB4503308, Installed on: 2019/09/02
KB4504282, Installed on: 2020/02/13
KB4504351, Installed on: 2020/02/13
KB4508433, Installed on: 2019/07/31
KB4515383, Installed on: 2019/09/23
KB4516115, Installed on: 2019/09/23
KB4517245, Installed on: 2019/11/20
KB4520390, Installed on: 2019/10/04
KB4521863, Installed on: 2019/10/10
KB4524244, Installed on: 2020/02/13
KB4524569, Installed on: 2019/11/18
KB4525419, Installed on: 2019/11/12
KB4528759, Installed on: 2020/01/15
KB4537759, Installed on: 2020/02/13
KB4538674, Installed on: 2020/02/13
KB4541338, Installed on: 2020/03/13
KB4552152, Installed on: 2020/04/16
KB4552931, Installed on: 2020/05/15
KB4560959, Installed on: 2020/06/16
KB4561600, Installed on: 2020/06/16
```

48337 - Windows ComputerSystemProduct Enumeration (WMI)

Synopsis

It is possible to obtain product information from the remote host using WMI.

Description

By querying the WMI class 'Win32_ComputerSystemProduct', it is possible to extract product information about the computer system such as UUID, IdentifyingNumber, vendor, etc.

See Also

http://www.nessus.org/u?a21ce849

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/08/16, Modification date: 2020/06/23

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
+ Computer System Product
  - IdentifyingNumber : VMware-ea 03 1a 42 4a b7 25 6b-dc 87 98 a0 20 4c 73 0c
  - Description       : Computer System Product
  - Vendor            : VMware, Inc.
  - Name              : VMware Virtual Platform
  - UUID              : 421A03EA-B74A-6B25-DC87-98A0204C730C
  - Version           : None
```

92433 - Terminal Services History

Synopsis

Nessus was able to gather terminal service connection information.

Description

Nessus was able to generate a report on terminal service connections on the target system.

See Also

http://www.nessus.org/u?15f94efb

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2018/11/15

Ports

vda-it-ts (TCP/0) Vulnerability State: Resurfaced

```
 Terminal Services Client
  - EDENBROWN.UK\t.styles
  - EDENBROWN.UK\t.styles
  - EDENBROWN.UK\t.styles
  - EDENBROWN.UK\t.styles
  - EDENBROWN.UK\t.styles
  - EDENBROWN.UK\t.styles
  - EDENBROWN.UK\t.styles
  - EDENBROWN.UK\t.styles
  - EDENBROWN.UK\t.styles
  - EDENBROWN.UK\t.styles


Terminal Services Server
  - S-1-5-21-289213053-1965310637-929701000-43470
  - S-1-5-21-289213053-1965310637-929701000-43470
  - S-1-5-21-289213053-1965310637-929701000-43470
  - S-1-5-21-289213053-1965310637-929701000-43470
  - S-1-5-21-289213053-1965310637-929701000-43470
  - S-1-5-21-289213053-1965310637-929701000-43470
  - S-1-5-21-289213053-1965310637-929701000-43470
  - S-1-5-21-289213053-1965310637-929701000-43470
  - S-1-5-21-289213053-1965310637-929701000-43470
  - S-1-5-21-289213053-1965310637-929701000-43470
  - S-1-5-21-289213053-1965310637-929701000-43470
```

```
  - S-1-5-21-289213053-1965310637-929701000-43470
  - S-1-5-21-289213053-1965310637-929701000-43470
  - S-1-5-21-289213053-1965310637-929701000-43470
  - S-1-5-21-289213053-1965310637-929701000-43470
  - S-1-5-21-289213053-1965310637-929701000-43470
  - S-1-5-21-289213053-1965310637-929701000-43470
  - S-1-5-21-289213053-1965310637-929701000-43470
  - S-1-5-21-289213053-1965310637-929701000-43470
  - S-1-5-21-289213053-1965310637-929701000-43470
  - S-1-5-21-289213053-1965310637-929701000-43470
  - S-1-5-21-289213053-1965310637-929701000-43470
  - S-1-5-21-289213053-1965310637-929701000-43470
  - S-1-5-21-289213053-1965310637-929701000-43470
  - S-1-5-21-289213053-1965310637-929701000-43470
  - S-1-5-21-289213053-1965310637-929701000-43470
  - S-1-5-21-289213053-1965310637-929701000-43470
  - S-1-5-21-289213053-1965310637-929701000-43470
  - S-1-5-21-289213053-1965310637-929701000-43470
  - S-1-5-21-289213053-1965310637-929701000-43470
  - S-1-5-21-289213053-1965310637-929701000-43470
  - S-1-5-21-289213053-1965310637-929701000-43470
  - S-1-5-21-289213053-1965310637-929701000-43470
  - S-1-5-21-289213053-1965310637-929701000-43470
  - S-1-5-21-289213053-1965310637-929701000-43470
  - [...]
```

10396 - Microsoft Windows SMB Shares Access

Synopsis

It is possible to access a network share.

Description

The remote has one or more Windows shares that can be accessed through the network with the given credentials. Depending on the share rights, it may allow an attacker to read / write confidential data.

Solution

To restrict access under Windows, open Explorer, do a right click on each share, go to the 'sharing' tab, and click on 'permissions'.

Risk Factor

None

Plugin Information:

Publication date: 2000/05/09, Modification date: 2020/03/09

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
The following shares can be accessed  :

- ADMIN$  - (readable,writable)
  + Content of this share :
..
$Reconfig$
ADAM
addins
ADFS
AdminArsenal
appcompat
apppatch
AppReadiness
assembly
autologon.log
AxInstSV
bcastdvr
bfsvc.exe
BitLockerDiscoveryVolumeContents
Boot
bootstat.dat
Branding
CbsTemp
Cluster
comsetup.log
Containers
```

```
CryptoGuard
CSC
Cursors
debug
diagerr.xml
diagnostics
DiagTrack
diagwrn.xml
DigitalLocker
Downloaded Installations
Downloaded Program Files
DtcInstall.log
ehome
ELAMBKUP
en-GB
en-US
explorer.exe
Fonts
GameBarPresenceWriter
Globalization
Help
HelpPane.exe
hh.exe
IdentityCRL
IE10_main.log
IE11_main.log
IE9_main.log
iis.log
IME
ImmersiveControlPanel
INF
InfusedApps
InputMethod
Installer
L2Schemas
LanguageOverlayCache
LiveKernelReports
Logs
Media
mib.bin
Microsoft.NET
Migration
Minidump
ModemLogs
msdfmap.ini
msxml4-KB954430-enu.LOG
msxml4-KB973688-enu.LOG
notepad.exe
OCR
ODBC.INI
ODBCINST.INI
Offline Address Books
Offline Web Pages
Patches
PCHEALTH
Performance
PFRO.log
PLA
PolicyDefinitions
Prefetch
PrintDialog
Professional.xml
progress.ini
Provisioning
regedit.exe
Registration

- C$  - (readable,writable)
  + Content of this share :
$Recycle.Bin
$WINRE_BACKUP_PARTITION.MARKER
.apdisk
.rnd
.TemporaryItems
._.apdisk
```

```
.__.TemporaryItems
2f7f73a2e6882176b3b1c4b5de71bee3
9794dad44e4e50dfe85be8ecbeb70155
ADCourier
Applied PowerBI Source
aspnet45_vb
Binaries
BOOTNXT
COMENSURA
Config.Msi
convrcfg.xml
d14c8f730fe2bb1038f3
db_backups
Documents and Settings
inetpub
KVRT_Data
MAT
MetaCompliance
Microsoft
msdia80.dll
MSOCache
Murach
OneDriveTemp
pagefile.sys
PerfLogs
Program Files
Program Files (x86)
ProgramData
Recovery
Reports
Screen savers
Self-Bill Converter OLD DNU - see source control
SQL Workplaces
SSMSTools
swapfile.sys
System Volume Information
temp
ualoc.inf
uasloc.inf
Users
Windows

- D$  - (readable,writable)
  + Content of this share :
OneDriveFiles
OneDriveTemp
Outlook Files
PowerBI
System Volume Information
```

52001 - WMI QuickFixEngineering (QFE) Enumeration

Synopsis

The remote Windows host has quick-fix engineering updates installed.

Description

By connecting to the remote host with the supplied credentials, this plugin enumerates quick-fix engineering updates installed on the remote host via WMI.

See Also

http://www.nessus.org/u?0c4ec249

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/02/16, Modification date: 2020/06/23

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
Here is a list of quick-fix engineering updates installed on the
remote system :

+ KB4552931
  - Description : Update
  - InstalledOn : 5/15/2020

+ KB4493478
  - Description : Security Update
  - InstalledOn : 8/5/2019

+ KB4497165
  - Description : Update
  - InstalledOn : 6/2/2020

+ KB4503308
  - Description : Security Update
  - InstalledOn : 9/2/2019

+ KB4508433
  - Description : Security Update
  - InstalledOn : 7/31/2019

+ KB4515383
  - Description : Security Update
  - InstalledOn : 9/23/2019

+ KB4516115
  - Description : Security Update
  - InstalledOn : 9/23/2019

+ KB4517245
  - Description : Update
  - InstalledOn : 11/20/2019

+ KB4520390
  - Description : Security Update
  - InstalledOn : 10/4/2019

+ KB4521863
  - Description : Security Update
  - InstalledOn : 10/10/2019

+ KB4524244
  - Description : Security Update
  - InstalledOn : 2/13/2020

+ KB4524569
  - Description : Security Update
  - InstalledOn : 11/18/2019

+ KB4525419
  - Description : Security Update
  - InstalledOn : 11/12/2019

+ KB4528759
  - Description : Security Update
  - InstalledOn : 1/15/2020

+ KB4537759
  - Description : Security Update
  - InstalledOn : 2/13/2020

+ KB4538674
  - Description : Security Update
  - InstalledOn : 2/13/2020

+ KB4541338
  - Description : Security Update
  - InstalledOn : 3/13/2020

+ KB4552152
  - Description : Security Update
```

```
  - InstalledOn : 4/16/2020

+ KB4560959
  - Description : Security Update
  - InstalledOn : 6/16/2020

+ KB4561600
  - Description : Security Update
  - InstalledOn : 6/16/2020

+ KB4560960
  - Description : Update
  - InstalledOn : 6/16/2020

Note that for detailed information on installed QFE's such as InstalledBy, Caption,
and so on, please run the scan with 'Report Verbosity' set to 'verbose'.
```

96534 - Firefox Browser Extension Enumeration

Synopsis

One or more Firefox browser extensions are installed on the remote host.

Description

Nessus was able to enumerate Firefox browser extensions installed on the remote host.

See Also

https://addons.mozilla.org/en-US/firefox/

Solution

Make sure that the use and configuration of these extensions comply with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Publication date: 2017/01/16, Modification date: 2020/06/23

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
User : Tim
|- Browser : Firefox
  |- Extension information :

    Name         : Default
    Description  : The default theme.
    Version      : 26.0
    Install Date : Jan. 13, 2014 at 12:35:15 GMT
    Update Date  : Jan. 13, 2014 at 12:35:15 GMT
    Path         : C:\Program Files (x86)\Mozilla Firefox\browser\extensions\{972ce4c6-7e08-4474-
a285-3208198ce6fd}
    ID           : {972ce4c6-7e08-4474-a285-3208198ce6fd}
    Note         : The file indicated by 'Path' was not found at the path specified. The extension
 may have been updated or removed since extensions.json was last updated.
    Status       : Enabled

    Name         : PDF Viewer
    Description  : Uses HTML5 to display PDF files directly in Firefox.
    Version      : 0.8.649
    Install Date : Jan. 15, 2014 at 11:39:04 GMT
    Update Date  : Jan. 15, 2014 at 11:39:04 GMT
    Path         : C:\Users\Tim\AppData\Roaming\Mozilla\Firefox\Profiles\5q5lmuju.default
\extensions\uriloader@pdf.js.xpi
    ID           : uriloader@pdf.js
    Status       : Enabled

    Name         : iMacros for Firefox
    Description  : Automate your web browser. Record and replay repetitious work.
    Version      : 8.6.0
    Install Date : Jan. 13, 2014 at 12:36:54 GMT
    Update Date  : Jan. 13, 2014 at 12:36:54 GMT
```

```
    Path         : C:\Users\Tim\AppData\Roaming\Mozilla\Firefox\Profiles\5q5lmuju.default
\extensions\{81BF1D23-5F17-408D-AC6B-BD6DF7CAF670}
    ID           : {81BF1D23-5F17-408D-AC6B-BD6DF7CAF670}
    Note         : The file indicated by 'Path' was not found at the path specified. The extension
 may have been updated or removed since extensions.json was last updated.
    Status       : Enabled

  |- Plugin information :

    Name        : Microsoft Office 2010
    Description : Office Authorization plug-in for NPAPI browsers
    Version     : 14.0.4730.1010
    Update Date : Jan.  9, 2010 at 21:42:18 GMT
    Path        : C:\PROGRA~2\MICROS~1\Office14\NPAUTHZ.DLL

    Name        : Microsoft Office 2010
    Description : The plug-in allows you to open and [...]
```

27524 - Microsoft Office Detection

Synopsis

The remote Windows host contains an office suite.

Description

Microsoft Office is installed on the remote host.

See Also

https://products.office.com/en-US/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/10/23, Modification date: 2020/06/23

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
The remote host has the following Microsoft Office 365 components installed :

  - Word : 16.0.12624.20466
  - Excel : 16.0.12624.20466
  - PowerPoint : 16.0.12624.20466
```

64582 - Netstat Connection Information

Synopsis

Nessus was able to parse the results of the 'netstat' command on the remote host.

Description

The remote host has listening ports or established connections that Nessus was able to extract from the results of the 'netstat' command.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/02/13, Modification date: 2018/05/16

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
 tcp4 (listen)
  src: [host=0.0.0.0, port=135]
  dst: [host=0.0.0.0, port=0]
```

```
tcp4 (listen)
  src: [host=0.0.0.0, port=445]
  dst: [host=0.0.0.0, port=0]

tcp4 (listen)
  src: [host=0.0.0.0, port=1801]
  dst: [host=0.0.0.0, port=0]

tcp4 (listen)
  src: [host=0.0.0.0, port=2103]
  dst: [host=0.0.0.0, port=0]

tcp4 (listen)
  src: [host=0.0.0.0, port=2105]
  dst: [host=0.0.0.0, port=0]

tcp4 (listen)
  src: [host=0.0.0.0, port=2107]
  dst: [host=0.0.0.0, port=0]

tcp4 (listen)
  src: [host=0.0.0.0, port=3389]
  dst: [host=0.0.0.0, port=0]

tcp4 (listen)
  src: [host=0.0.0.0, port=5040]
  dst: [host=0.0.0.0, port=0]

tcp4 (listen)
  src: [host=0.0.0.0, port=49664]
  dst: [host=0.0.0.0, port=0]

tcp4 (listen)
  src: [host=0.0.0.0, port=49665]
  dst: [host=0.0.0.0, port=0]

tcp4 (listen)
  src: [host=0.0.0.0, port=49666]
  dst: [host=0.0.0.0, port=0]

tcp4 (listen)
  src: [host=0.0.0.0, port=49669]
  dst: [host=0.0.0.0, port=0]

tcp4 (listen)
  src: [host=0.0.0.0, port=49670]
  dst: [host=0.0.0.0, port=0]

tcp4 (listen)
  src: [host=0.0.0.0, port=49671]
  dst: [host=0.0.0.0, port=0]

tcp4 (listen)
  src: [host=0.0.0.0, port=49685]
  dst: [host=0.0.0.0, port=0]

tcp4 (listen)
  src: [host=0.0.0.0, port=49695]
  dst: [host=0.0.0.0, port=0]

tcp4 (listen)
  src: [host=0.0.0.0, port=49698]
  dst: [host=0.0.0.0, port=0]

tcp4 (listen)
  src: [host=0.0.0.0, port=49704]
  dst: [host=0.0.0.0, port=0]

tcp4 (listen)
  src: [host=0.0.0.0, port=55507]
  dst: [host=0.0.0.0, port=0]

tcp4 (listen)
  src: [host=0.0.0.0, port=60168]
  dst: [host=0.0.0.0, port=0]
```

```
tcp4 (listen)
  src: [host=10.0.100.4, port=139]
  dst: [host=0.0.0.0, port=0]

tcp4 (established)
  src: [host=10.0.100.4, port=3389]
  dst: [host=10.0.103.105, port=50331]

tcp4 (established)
  src: [host=10.0.100.4, port=49760]
  dst: [host=10.0.0.223, port=49159]

tcp4 (established)
  src: [host=10.0.100.4, port=49791]
  dst: [host=51.141.111.10, port=443]

tcp4 (established)
  src: [host=10.0.100.4, port=49797]
  dst: [host=52.109.28.2, port=443]

tcp4 (established)
 [...]
```

92424 - MUICache Program Execution History

Synopsis

Nessus was able to enumerate recently executed programs on the remote host.

Description

Nessus was able to query the MUIcache registry key to find evidence of program execution.

See Also

https://forensicartifacts.com/2010/08/registry-muicache/

http://windowsir.blogspot.com/2005/12/mystery-of-muicachesolved.html

http://www.nirsoft.net/utils/muicache_view.html

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2018/05/16

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
 c:\users\t.styles\appdata\roaming\parallels\shared applications\safari
 (mac).exe.applicationcompany : Parallels Software International, Inc.
c:\users\t.styles\appdata\roaming\parallels\shared applications\grapher
 (mac).exe.applicationcompany : Parallels Software International, Inc.
c:\users\t.styles\appdata\roaming\parallels\shared applications\itunes (mac).exe.friendlyappname :
 iTunes (Mac)
c:\program files\microsoft office\office14\visio.exe.friendlyappname : Microsoft Visio
c:\program files (x86)\notepad++\notepad++.exe.applicationcompany : Don HO don.h@free.fr
c:\users\t.styles\appdata\roaming\parallels\shared applications\grab
 (mac).exe.applicationcompany : Parallels Software International, Inc.
c:\program files (x86)\microsoft visual studio 10.0\common7\ide\devenv.exe.friendlyappname :
 Microsoft Visual Studio 2010
c:\users\t.styles\appdata\roaming\parallels\shared applications\evernote
 (mac).exe.applicationcompany : Parallels Software International, Inc.
c:\users\t.styles\appdata\roaming\parallels\shared applications\preview
 (mac).exe.applicationcompany : Parallels Software International, Inc.
c:\users\t.styles\appdata\roaming\parallels\shared applications\reminders
 (mac).exe.applicationcompany : Parallels Software International, Inc.
c:\users\t.styles\appdata\roaming\parallels\shared applications\calendar
 (mac).exe.friendlyappname : Calendar (Mac)
c:\users\t.styles\appdata\roaming\parallels\shared applications\ibooks (mac).exe.friendlyappname :
 iBooks (Mac)
```

```
c:\program files\internet explorer\iexplore.exe.applicationcompany : Microsoft Corporation
c:\users\t.styles\appdata\roaming\parallels\shared applications\system information
 (mac).exe.friendlyappname : System Information (Mac)
c:\windows\system32\explorerframe.dll.friendlyappname : ExplorerFrame
c:\users\t.styles\appdata\roaming\parallels\shared applications\dvd player
 (mac).exe.applicationcompany : Parallels Software International, Inc.
c:\program files\microsoft office\office14\visio.exe.applicationcompany : Microsoft [...]
```

92417 - Direct3D Recent Program

Synopsis

Nessus was able to enumerate the most recent program to use Direct3D for each user on the remote host.

Description

Nessus was able to query the registry to find the most recent program to use Direct3D for each user on the remote Windows host.

See Also

http://www.nessus.org/u?e275bc08

http://www.nessus.org/u?7def0916

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2018/11/15

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
.DEFAULT
  - TeamViewer_Service.exe

S-1-5-18
  - TeamViewer_Service.exe
```

48942 - Microsoft Windows SMB Registry : OS Version and Processor Architecture

Synopsis

It was possible to determine the processor architecture, build lab strings, and Windows OS version installed on the remote system.

Description

Nessus was able to determine the processor architecture, build lab strings, and the Windows OS version installed on the remote system by connecting to the remote registry with the supplied credentials.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/08/31, Modification date: 2020/01/22

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Operating system version = 10.18363
Architecture = x64
Build lab extended = 18362.1.amd64fre.19h1_release.190318-1202
```

45051 - WMI Antivirus Enumeration

Synopsis

It is possible to obtain the list of antivirus software installed on the remote Windows host.

Description

By connecting to the remote Windows host with the supplied credentials, this plugin uses WMI to enumerate antivirus software installed on it.
Note that this plugin extracts this information from the 'root\securitycenter' and 'root\securitycenter2' WMI namespaces, which are only available in Windows desktop operating systems such as XP, Vista and Windows 7.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/03/12, Modification date: 2020/06/23

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
Here is the list of anti-virus software registered under the
'root\SecurityCenter2' WMI namespace :

+ Sophos Anti-Virus

  - pathToSignedProductExe : C:\Program Files (x86)\Sophos\Sophos Anti-Virus\WSCClient.exe
  - pathToSignedReportingExe : C:\Program Files (x86)\Sophos\Sophos Anti-Virus\WSCClient.exe
  - productState : 331776

+ Windows Defender

  - pathToSignedProductExe : windowsdefender://
  - pathToSignedReportingExe : %ProgramFiles%\Windows Defender\MsMpeng.exe
  - productState : 393472
```

92418 - Windows Explorer Typed Paths

Synopsis

Nessus was able to enumerate the directory paths that users visited by typing the full directory path into Windows Explorer.

Description

Nessus was able to enumerate the directory paths that users visited by manually typing the full directory path into Windows Explorer. The generated folder list report contains folders local to the system, folders from past mounted network drives, and folders from mounted devices.

See Also

http://www.nessus.org/u?f92f6e9f

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2018/11/15

Ports

vda-it-ts (TCP/0) Vulnerability State: Resurfaced

```
V:\
\\oak\report
V:\Data\BRData
\\data01\brdirectors

Extended explorer typed paths report attached.
```

136515 - Security Updates for Microsoft Visual Studio Products (May 2020)

Synopsis

The Microsoft Visual Studio Products are affected by multiple vulnerabilities.

Description

The Microsoft Visual Studio Products are missing security updates. It is, therefore, affected by multiple vulnerabilities :
- A denial of service vulnerability exists when .NET Core or .NET Framework improperly handles web requests. An attacker who successfully exploited this vulnerability could cause a denial of service against a .NET Core or .NET Framework web application. The vulnerability can be exploited remotely, without authentication. (CVE-2020-1108)
- A denial of service vulnerability exists when ASP.NET Core improperly handles web requests. An attacker who successfully exploited this vulnerability could cause a denial of service against an ASP.NET Core web application. The vulnerability can be exploited remotely, without authentication. (CVE-2020-1161)

Solution

Microsoft has released the following security updates to address this issue:
- Update 15.9.23 for Visual Studio 2017
- Update 16.0.14 for Visual Studio 2019
- Update 16.4.8 for Visual Studio 2019
- Update 16.5.5 for Visual Studio 2019

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

6.1

CVSS v3.0 Base Score

7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.5 (E:U/RL:O/RC:C)

CVSS Base Score

5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS Temporal Score

3.7 (E:U/RL:OF/RC:C)

References

CVE	CVE-2020-1108
CVE	CVE-2020-1161

Plugin Information:

Publication date: 2020/05/12, Modification date: 2020/06/08

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
  Path              : C:\Program Files (x86)\Microsoft Visual Studio\2017\Community\Common7\IDE
\devenv.exe
  Installed version : 15.9.28307.1093
  Fixed version     : 15.9.28307.1146
```

11777 - Microsoft Windows SMB Share Hosting Possibly Copyrighted Material

Synopsis

The remote host may contain material (movies/audio) infringing copyright.

Description

This plugin displays a list of media files (such as .mp3, .ogg, .mpg, .avi) which have been found on the remote SMB shares.
Some of these files may contain copyrighted materials, such as commercial movies or music files, that are being shared without the owner's permission.
If any of these files actually contain copyrighted material, and if they are freely swapped around, your organization might be held liable for copyright infringement by associations such as the RIAA or the MPAA.

Solution

Delete the files infringing copyright.

Risk Factor

None

Plugin Information:

Publication date: 2003/06/26, Modification date: 2012/11/29

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Here is a list of files which have been found on the remote SMB shares.
Some of these files may contain copyrighted materials, such as commercial
movies or music files.

 + C$ :

\Program Files\WindowsApps\Microsoft.XboxGamingOverlay_5.220.4292.0_x64__8wekyb3d8bbwe\Assets
\Sounds\Message_Notification_SetA_v14_v2.mp3
\Program Files\WindowsApps\Microsoft.XboxGamingOverlay_5.220.4292.0_x64__8wekyb3d8bbwe\Assets
\Sounds\Group_Voice_Exit_Others_SetA_v1.mp3
\Program Files\WindowsApps\Microsoft.XboxGamingOverlay_5.220.4292.0_x64__8wekyb3d8bbwe\Assets
\Sounds\Group_Voice_Exit_Me_SetA_v1.mp3

\Program Files\WindowsApps\Microsoft.XboxApp_48.65.22001.0_x64__8wekyb3d8bbwe\Assets
\AchievementUnlocked.mp3
\Program Files\WindowsApps\Microsoft.XboxGamingOverlay_5.220.4292.0_x64__8wekyb3d8bbwe\Assets
\Sounds\AchievementUnlocked.mp3
\Program Files\WindowsApps\Microsoft.XboxGamingOverlay_5.220.4292.0_x64__8wekyb3d8bbwe\Assets
\Sounds\Group_Voice_Entry_Me_SetA_v1.mp3
\Program Files\WindowsApps\Microsoft.XboxGamingOverlay_5.220.4292.0_x64__8wekyb3d8bbwe\Assets
\Sounds\Group_Voice_Entry_Others_SetA_v1.mp3
\Program Files (x86)\Android\android-sdk\platforms\android-27\data\res\raw\fallbackring.ogg

\Program Files\WindowsApps\Microsoft.ZuneVideo_10.20032.16211.0_x64__8wekyb3d8bbwe\Assets
\ImmersiveControl_Slider_Click_Sound.wma
\Program Files\WindowsApps\Microsoft.ZuneVideo_10.20022.11011.0_x64__8wekyb3d8bbwe\Assets
\ImmersiveControl_Slider_Click_Sound.wma
\Program Files\WindowsApps\Microsoft.Windows.Photos_2020.19111.24110.0_x64__8wekyb3d8bbwe\AppCS
\Assets\ModularMusic\Classic_00\music_Neutral_01_LOOP_D.wma
\Program Files\WindowsApps\Microsoft.Windows.Photos_2020.19111.24110.0_x64__8wekyb3d8bbwe\AppCS
\Assets\ModularMusic\Classic_00\music_Neutral_01_LOOP_C.wma
\Program Files\WindowsApps\Microsoft.Windows.Photos_2020.19111.24110.0_x64__8wekyb3d8bbwe\AppCS
\Assets\ModularMusic\Classic_00\music_Neutral_01_LOOP_B.wma
\Program [...]
```

124120 - Microsoft Outlook Attachment Previewing Enabled

Synopsis

Microsoft Outlook application that is installed on the remote host has attachment previewing enabled.

Description

Microsoft Outlook application that is installed on the remote host has attachment previewing enabled.

Solution

Disable attachment previewing settings.

Risk Factor

None

Plugin Information:

Publication date: 2019/04/17, Modification date: 2019/04/17

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
Outlook application in Microsoft Office 2010 has attachment previewing enabled.
Outlook application in Microsoft Office 2016 has attachment previewing enabled.
```

24272 - Network Interfaces Enumeration (WMI)

Synopsis

Nessus was able to obtain the list of network interfaces on the remote host.

Description

Nessus was able, via WMI queries, to extract a list of network interfaces on the remote host and the IP addresses attached to them.
Note that this plugin only enumerates IPv6 addresses for systems running Windows Vista or later.

See Also

http://www.nessus.org/u?b362cab2

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/02/03, Modification date: 2020/06/23

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
+ Network Interface Information :

 - Network Interface = [00000001] vmxnet3 Ethernet Adapter
 - MAC Address = 00:50:56:A6:49:57
 - IPAddress/IPSubnet = 10.0.100.4/255.255.0.0
 - IPAddress/IPSubnet = fe80::f804:cc4d:d598:807c/64


+ Routing Information :

    Destination     Netmask         Gateway
    -----------     -------         -------
    0.0.0.0         0.0.0.0         10.0.0.1
    10.0.0.0        255.255.0.0     0.0.0.0
    10.0.100.4      255.255.255.255 0.0.0.0
    10.0.255.255    255.255.255.255 0.0.0.0
    127.0.0.0       255.0.0.0       0.0.0.0
    127.0.0.1       255.255.255.255 0.0.0.0
    127.255.255.255 255.255.255.255 0.0.0.0
    224.0.0.0       240.0.0.0       0.0.0.0
    224.0.0.0       240.0.0.0       0.0.0.0
    255.255.255.255 255.255.255.255 0.0.0.0
    255.255.255.255 255.255.255.255 0.0.0.0
```

92425 - Microsoft Office File History

Synopsis

Nessus was able to enumerate files opened in Microsoft Office on the remote host.

Description

Nessus was able to gather evidence of files that were opened using any Microsoft Office application. The report was extracted from Office MRU (Most Recently Used) registry keys.

See Also

https://products.office.com/en-US/

https://www.taksati.org/mru/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2018/11/15

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
 item 37
item 32
```

```
    item 28
    item 15
    item 4
    item 16
    item 48
    item 42
    item 19
    item 10
    item 27
    item 21
    max display
    item 34
    item 24
    item 6
    item 50
    item 40
    item 35
    item 31
    item 18
    item 45
    item 49
    item 29
    item 8
    item 2
    item 41
    item 3
    item 43
    item 13
    item 1
    item 38
    item 36
    item 17
    item 11
    item 26
    item 5
    item 20
    item 46
    item 39
    item 30
    item 7
    item 12
    item 23
    item 22
    item 47
    item 44
    item 14
    item 25
    item 9
    item 33
    item 37
    item 32
    item 28
    item 15
    item 4
    item 16
    item 48
    item 42
    item 19
    item 10
    item 27
    item 21
    max display
    item 34
    item 24
    item 6
    item 50
    item 40
    item 35
    item 31
    item 18
    item 45
    item 49
    item 29
    item 8
    item 2
```

```
folderid_documents
folderid_desktop
item 41
item 3
item 43
item 13
item 1
item 38
item 36
item 17
item 11
item 26
item 5
item 20
item 46
item 39
item 30
item 7
item 12
item 23
item 22
item 47
item 44
item 14
item 25
item 9
item 33
item 37
item 32
item 28
item 15
item 51
item 4
item 16
item 48
item 42
item 19
item 10
item 27
item 21
max display
item 34
item 24
item 6
item 50
item 40
item 35
item 31
item 18
item 45
item 49
item 29
item 8
item 2
folderid_documents
folderid_desktop
item 41
item 3
item 43
item 13
item 1
item 38
item 36
item 17
item 11
item 26
item 5
item 20
item 46
item 39
item 30
item 7
item 12
item 23
item 22
```

```
item 47
item 44
item 14
item 25
item 9
item 33
item 20
item 1
item 2
item 3
item 25
item 14
item 28
item 22
item 16
item 4
item 23
item 18
item 6
item 5
item 13
item 12
item 9
item 8
item 11
item 29
item 27
item 17
item 26
item 19
item 24
item 21
item 15
item 10
item 7
item 30
item 37
item 32
item 28
item 15
item 4
item 16
item 48
item 42
item 19
item 10
item 27
item 21
max display
item 34
item 24
item 6
item 50
item 40
item 35
item 31
item 18
item 45
item 49
item 29
item 8
item 2
item 41
item 3
item 43
item 13
item 1
item 38
item 36
item 17
item 11
item 26
item 5
item 20
item 46
```

```
item 39
item 30
item 7
item 12
item 23
item 22
item 47
item 44
item 14
item 25
item 9
item 33
item 32
item 37
item 28
item 15
item 4
item 16
item 42
item 48
item 19
item 10
item 27
max display
item 21
item 34
item [...]
```

92423 - Windows Explorer Recently Executed Programs

Synopsis

Nessus was able to enumerate recently executed programs on the remote host.

Description

Nessus was able to find evidence of program execution using Windows Explorer registry logs and settings.

See Also

http://www.forensicswiki.org/wiki/LastVisitedMRU

http://www.nessus.org/u?7e00b191

http://www.nessus.org/u?ac4dd3fb

http://www.nessus.org/u?c409cb41

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2019/08/15

Ports

vda-it-ts (TCP/0) Vulnerability State: Resurfaced

```
 DTSWizard.exePO :i+00.9#K&]B_
{22124D62-F9DC-4762-8B7A-7CC7B355446F}:DGYr?DUk0&&7{GQ<*Q<*tFCFSF@1OneDrive - nGAGE
 Specialist Recruitment Limited 1tY^Hg3(gVAGk .OneDrive - nGAGE Specialist Recruitment Limited
 1lV1PowerBI@ .PowerBIn1PV0CRM_AC~1J P<PV.xO(eCRM_Activity)
Teams.exeDGYr?DUk0tFCFSF@1OneDrive - nGAGE Specialist Recruitment Limited 1tY^Hg3(gVAGk .OneDrive
 - nGAGE Specialist Recruitment Limited 1lV1PowerBI@ .PowerBIn1Pt0CRM_AC~1J P<Pt.xOpCRM_Activity)
PickerHost.exe:DGYr?DUk0&&7{GQ<*Q<*tFCFSF@1OneDrive - nGAGE Specialist Recruitment Limited
 1tY^Hg3(gVAGk .OneDrive - nGAGE Specialist Recruitment Limited 1lV1PowerBI@ .PowerBIh1Proactive
 C&WL .Proactive C&Wf1PFZ0BrandingB P;PFZ./?Branding)
Evernote.exePO :i+00.+ezFkp:
{393DA269-CCA8-4404-842C-D08AA3887E55}:DGYr?DUk0&&7{GQ<*Q<*tFCFSF@1OneDrive - nGAGE
 Specialist Recruitment Limited 1tY^Hg3(gVAGk .OneDrive - nGAGE Specialist Recruitment Limited
 1lV1PowerBI@ .PowerBIn1PF0CRM_AC~1J P<PF.xO{CRM_Activity)
SQLyog.exePO :i+00.+ezFkp:
 \n\r
```

```
{1EFA9EA3-BF88-478A-B1C8-7BB07B259D2D}PO :i+00/C:\x1P,Usersd sN$P,.
%JB:OUsers@shell32.dll,-21813\1PTFF34~1.STYB NEP.}\nd3t.styles1P1ONEDRI~1 H`P.vxpROneDrive -
 nGAGE Specialist Recruitment Limited 1b1PW4PowerBI@ ;N|PW4.a`TPowerBI)n1P\rn0CRM_AC~1J P<P
\rn.xO>PCRM_Activity)
Power BI Helper Application.exe:B'l r&&1kwSkwSkb1P<PowerBI@ ;N|P<.aJPowerBI)n1PU0CRM_AC~1J P<PU.xO
\nCRM_Activity)
VISIO.EXE:B'l r&&1kwSkwSkV1PYCovid19@ }PyPY.M!Covid19
devenv.exePO :i+00.:$i0EAz
{6519CB88-B091-47F9-9CB0-2018D0921EA3}PO :i+00/H:\n10P\rTActive ProjectsP jHP\rT.^Active
 ProjectsH1PfAI6 JM\n]Pf.*)AI
{02829E3F-C6C2-4CB9-B72A-18B8E77C3EEC}PO :i+00/C:\x1P,Usersd sN$P,.
%JB:OUsers@shell32.dll,-21813\1PTFF34~1.STYB NEP.}\nd3t.styles1P441ONEDRI~1 H`P44.vxpOneDrive -
 nGAGE Specialist Recruitment Limited 1b1PW4PowerBI@ ;N|PW4.a`TPowerBI)p1Pj40PROACT~1L PK4Pj4.R-
$Proactive C&W)p1P4DOCUME~1L P4P4.H 9JDocumentation)
AcroRd32.exePO [...]
```

58651 - Netstat Active Connections

Synopsis

Active connections are enumerated via the 'netstat' command.

Description

This plugin runs 'netstat' on the remote machine to enumerate all active 'ESTABLISHED' or 'LISTENING' tcp/udp connections.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2012/04/10, Modification date: 2018/06/19

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
Netstat output :

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       448
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:1801           0.0.0.0:0              LISTENING       4248
  TCP    0.0.0.0:2103           0.0.0.0:0              LISTENING       4248
  TCP    0.0.0.0:2105           0.0.0.0:0              LISTENING       4248
  TCP    0.0.0.0:2107           0.0.0.0:0              LISTENING       4248
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       1032
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       3584
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       748
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       588
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       2000
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       2488
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING       3688
  TCP    0.0.0.0:49671          0.0.0.0:0              LISTENING       748
  TCP    0.0.0.0:49685          0.0.0.0:0              LISTENING       3172
  TCP    0.0.0.0:49695          0.0.0.0:0              LISTENING       1660
  TCP    0.0.0.0:49698          0.0.0.0:0              LISTENING       4248
  TCP    0.0.0.0:49704          0.0.0.0:0              LISTENING       712
  TCP    0.0.0.0:55507          0.0.0.0:0              LISTENING       1604
  TCP    0.0.0.0:60168          0.0.0.0:0              LISTENING       11556
  TCP    10.0.100.4:139         0.0.0.0:0              LISTENING       4
  TCP    10.0.100.4:3389        10.0.103.105:50331     ESTABLISHED     1032
  TCP    10.0.100.4:49760       10.0.0.223:49159       ESTABLISHED     3688
  TCP    10.0.100.4:49791       51.141.111.10:443      ESTABLISHED     157180
  TCP    10.0.100.4:49797       52.109.28.2:443        ESTABLISHED     157180
  TCP    10.0.100.4:49799       [...]
```

38689 - Microsoft Windows SMB Last Logged On User Disclosure

Synopsis

Nessus was able to identify the last logged on user on the remote host.

Description

By connecting to the remote host with the supplied credentials, Nessus was able to identify the username associated with the last successful logon.
Microsoft documentation notes that interactive console logons change the DefaultUserName registry entry to be the last logged-on user.

See Also

http://www.nessus.org/u?a29751b5

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/05/05, Modification date: 2019/09/02

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Last Successful logon : EDEN_MAIN\a.meek
```

57033 - Microsoft Patch Bulletin Feasibility Check

Synopsis

Nessus is able to check for Microsoft patch bulletins.

Description

Using credentials supplied in the scan policy, Nessus is able to collect information about the software and patches installed on the remote Windows host and will use that information to check for missing Microsoft security updates.
Note that this plugin is purely informational.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/06, Modification date: 2018/11/01

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Nessus is able to test for missing patches using :
  Nessus
```

51187 - WMI Encryptable Volume Enumeration

Synopsis

The remote Windows host has encryptable volumes available.

Description

By connecting to the remote host with the supplied credentials, this plugin enumerates encryptable volume information available on the remote host via WMI.

See Also

http://www.nessus.org/u?8aa7973e

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/12/15, Modification date: 2020/06/23

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
Here is a list of encryptable volumes available on the remote system :

+ DriveLetter C:

  - BitLocker Version : None
  - Conversion Status : Fully Decrypted
  - DeviceID : \\?\Volume{c7f38484-74b3-11e3-adb5-806e6f6e6963}\
  - Encryption Method : None
  - Identification Field : None
  - Key Protectors : None Found
  - Lock Status : Unlocked
  - Percentage Encrypted : 0.0%
  - PersistentVolumeID :
  - Protection Status : Protection Off
  - Size : 248.39 GB

+ DriveLetter D:

  - Automatic Unlock : Disabled
  - BitLocker Version : None
  - Conversion Status : Fully Decrypted
  - DeviceID : \\?\Volume{854947fd-0000-0000-0000-100000000000}\
  - Encryption Method : None
  - Identification Field : None
  - Key Protectors : None Found
  - Lock Status : Unlocked
  - Percentage Encrypted : 0.0%
  - PersistentVolumeID :
  - Protection Status : Protection Off
  - Size : 100.00 GB
```

44871 - WMI Windows Feature Enumeration

Synopsis

It is possible to enumerate Windows features using WMI.

Description

Nessus was able to enumerate the server features of the remote host by querying the 'Win32_ServerFeature' class of the '\Root\cimv2' WMI namespace for Windows Server versions or the 'Win32_OptionalFeature' class of the '\Root\cimv2' WMI namespace for Windows Desktop versions.
Note that Features can only be enumerated for Windows 7 and later for desktop versions.

See Also

https://msdn.microsoft.com/en-us/library/cc280268

https://docs.microsoft.com/en-us/windows/desktop/WmiSdk/querying-the-status-of-optional-features

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/02/24, Modification date: 2020/06/23

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
Nessus enumerated the following Windows features :

  - DirectoryServices-ADAM-Client
  - FaxServicesClientPackage
  - IIS-ASPNET
  - IIS-ASPNET45
  - IIS-ApplicationDevelopment
```

```
- IIS-CommonHttpFeatures
- IIS-DefaultDocument
- IIS-DirectoryBrowsing
- IIS-HttpErrors
- IIS-HttpRedirect
- IIS-IIS6ManagementCompatibility
- IIS-ISAPIExtensions
- IIS-ISAPIFilter
- IIS-LegacyScripts
- IIS-LegacySnapIn
- IIS-ManagementConsole
- IIS-ManagementScriptingTools
- IIS-ManagementService
- IIS-Metabase
- IIS-NetFxExtensibility
- IIS-NetFxExtensibility45
- IIS-RequestFiltering
- IIS-Security
- IIS-StaticContent
- IIS-WMICompatibility
- IIS-WebServer
- IIS-WebServerManagementTools
- IIS-WebServerRole
- Internet-Explorer-Optional-amd64
- MSMQ-Container
- MSMQ-Server
- MSRDC-Infrastructure
- MediaPlayback
- Microsoft-Windows-Client-EmbeddedExp-Package
- Microsoft-Windows-NetFx3-OC-Package
- Microsoft-Windows-NetFx3-WCF-OC-Package
- Microsoft-Windows-NetFx4-US-OC-Package
- Microsoft-Windows-NetFx4-WCF-US-OC-Package
- MicrosoftWindowsPowerShellV2
- MicrosoftWindowsPowerShellV2Root
- NetFx3
- NetFx4-AdvSrvs
- NetFx4Extended-ASPNET45
- Printing-Foundation-Features
- Printing-Foundation-InternetPrinting-Client
- Printing-PrintToPDFServices-Features
- Printing-XPSServices-Features
- SMB1Protocol
- SMB1Protocol-Client
- SMB1Protocol-Deprecation
- SMB1Protocol-Server
- SearchEngine-Client-Package
- WAS-ConfigurationAPI
- WAS-ProcessModel
- WAS-WindowsActivationService
- WCF-MSMQ-Activation45
- WCF-Pipe-Activation45
- WCF-Services45
- WCF-TCP-Activation45
- WCF-TCP-PortSharing45
- Windows-Defender-Default-Definitions
- WindowsMediaPlayer
- WorkFolders-Client
```

92426 - OpenSaveMRU History

Synopsis

Nessus was able to enumerate opened and saved files on the remote host.

Description

Nessus was able to generate a report on files that were opened using the shell dialog box or saved using the shell dialog box. This is the box that appears when you attempt to save a document or open a document in Windows Explorer.

See Also

http://www.nessus.org/u?ac4dd3fb

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2018/05/23

Ports

vda-it-ts (TCP/0) Vulnerability State: Resurfaced

```
Open / Save report attached.
```

66542 - JavaScript Enabled in Adobe Reader

Synopsis

The remote Windows host has JavaScript enabled in Adobe Reader.

Description

JavaScript is enabled in Adobe Reader.
Note that Nessus can only check the SIDs of logged on users, and thus the results may be incomplete.

See Also

http://www.nessus.org/u?f30673d6

Solution

Disable JavaScript in Adobe Reader unless it is needed.

Risk Factor

None

Plugin Information:

Publication date: 2013/05/22, Modification date: 2013/05/22

Ports

vda-it-ts (TCP/445) Vulnerability State: Resurfaced

```
Nessus found JavaScript enabled for the following user and version
of Adobe Reader :

  Version DC for SID S-1-5-21-289213053-1965310637-929701000-34059
```

10395 - Microsoft Windows SMB Shares Enumeration

Synopsis

It is possible to enumerate remote network shares.

Description

By connecting to the remote host, Nessus was able to enumerate the network share names.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/05/09, Modification date: 2020/03/09

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Here are the SMB shares available on the remote host :

  - 2nd floor 222
  - ADMIN$
  - C$
  - D$
  - IPC$
  - print$
```

11217 - Microsoft SQL Server Detection (credentialed check)

Synopsis

The remote host has a database server installed.

Description

Nessus has detected one or more installs of Microsoft SQL server by examining the registry and file systems on the remote host.

See Also

https://azure.microsoft.com/en-us/?ocid=cloudplat_hp

Solution

Ensure the latest service pack and hotfixes are installed.

Risk Factor

None

Plugin Information:

Publication date: 2003/01/26, Modification date: 2019/11/22

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
  Version             : 12.0.4522.0 Express Edition
  Path                : C:\Program Files\Microsoft SQL Server\120\LocalDB\Binn\
  Named Instance      : MSSQL12E.LOCALDB
  Recommended Version : 12.0.5000 (2014 + SP2 (KB 3171021)).

 Express Edition
  Path                : C:\Program Files\Microsoft SQL Server\130\LocalDB\Binn\
  Named Instance      : MSSQL13E.LOCALDB
```

135592 - Oracle Java SE 1.7.0_261 / 1.8.0_251 / 1.11.0_7 / 1.14.0_1 Multiple Vulnerabilities (Apr 2020 CPU)

Synopsis

The remote host is affected by multiple vulnerabilities

Description

The version of Oracle (formerly Sun) Java SE or Java for Business installed on the remote host is prior to 7 Update 261, 8 Update 251, 11 Update 7, or 14 Update 1. It is, therefore, affected by multiple vulnerabilities related to the following components :
- Oracle Java SE and Java SE Embedded are prone to a buffer overflow attack, over 'Multiple' protocol.
This issue affects the 'JavaFX (libxslt)' component. Successful attacks of this vulnerability allow unauthenticated attacker with network access to takeover of Java SE. (CVE-2019-18197)
- Oracle Java SE and Java SE Embedded are prone to partial denial of service (partial DOS) vulnerability.
An unauthenticated remote attacker can exploit this over 'Multiple' protocol. This issue affects the 'Scripting' component. (CVE-2020-2754, CVE-2020-2755)
- Oracle Java SE and Java SE Embedded are prone to partial denial of service (partial DOS) vulnerability.
An unauthenticated remote attacker can exploit this over 'Multiple' protocol. This issue affects the 'Serialization' component. (CVE-2020-2756, CVE-2020-2757)
- Oracle Java SE prone to unauthorized read access vulnerability. An unauthenticated remote attacker can exploit this over 'Multiple' protocol can result in unauthorized read access to a subset of Java SE accessible data. This issue affects the 'Advanced Management Console' component. (CVE-2020-2764)
- Oracle Java SE and Java SE Embedded are prone to unauthorized write/read access vulnerability. An unauthenticated remote attacker over 'HTTPS' can read, update, insert or delete access to some of Java SE accessible data. This issue affects the 'JSSE' component. (CVE-2020-2767)
- Oracle Java SE and Java SE Embedded are prone to partial denial of service (partial DOS) vulnerability.
An unauthenticated remote attacker can exploit this over 'Multiple' protocol. This issue affects the 'Scripting' component. (CVE-2020-2773)
It is also affected by other vulnerabilities; please see vendor advisories for more information.
Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.oracle.com/a/tech/docs/cpuapr2020cvrf.xml

https://www.oracle.com/security-alerts/cpuapr2020.html

Solution

Upgrade to Oracle JDK / JRE 14 Update 1 , 11 Update 7, 8 Update 251 , 7 Update 261 or later.
If necessary, remove any affected versions.

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

7.3

CVSS v3.0 Base Score

4.8 (AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v3.0 Temporal Score

4.2 (E:U/RL:O/RC:C)

CVSS Base Score

5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)

CVSS Temporal Score

4.3 (E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2020-2805
CVE	CVE-2020-2816
CVE	CVE-2020-2757
CVE	CVE-2020-2756
CVE	CVE-2020-2767
CVE	CVE-2020-2778
CVE	CVE-2020-2800
CVE	CVE-2020-2803
CVE	CVE-2020-2764
CVE	CVE-2020-2830
CVE	CVE-2020-2755
CVE	CVE-2020-2754
CVE	CVE-2019-18197
CVE	CVE-2020-2781
CVE	CVE-2020-2773
XREF	IAVA:2020-A-0134

Plugin Information:

Publication date: 2020/04/16, Modification date: 2020/04/21

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
The following vulnerable instances of Java are installed on the
remote host :

  Path              : C:\Users\All Users\Oracle\Java\javapath_target_529031\java.exe
  Path              : C:\Documents and Settings\All Users\Oracle\Java\javapath\java.exe
  Path              : C:\Documents and Settings\All Users\Oracle\Java
\javapath_target_529031\java.exe
  Path              : C:\ProgramData\Oracle\Java\javapath\java.exe
  Path              : C:\ProgramData\Oracle\Java\javapath_target_529031\java.exe
  Path              : C:\Users\All Users\Oracle\Java\javapath\java.exe
  Installed version : 1.8.0_171
  Fixed version     : 1.7.0_261 / 1.8.0_251 / 1.11.0_7 / 1.14.0_1

  Path              : C:\Program Files\Java\jdk1.8.0_181\jre\bin\java.exe
  Path              : C:\Program Files\Java\jdk1.8.0_181\jre
  Path              : C:\Program Files (x86)\Java\jdk1.8.0_181\jre
  Path              : C:\Program Files (x86)\Java\jdk1.8.0_181\bin\java.exe
  Path              : C:\Program Files (x86)\Java\jdk1.8.0_181\jre\bin\java.exe
  Path              : C:\Program Files\Java\jdk1.8.0_181\bin\java.exe
  Installed version : 1.8.0_181
  Fixed version     : 1.7.0_261 / 1.8.0_251 / 1.11.0_7 / 1.14.0_1

  Path              : C:\Program Files\DBeaver\jre\bin\java.exe
  Installed version : 1.8.0_77
  Fixed version     : 1.7.0_261 / 1.8.0_251 / 1.11.0_7 / 1.14.0_1
```

111071 - Security Updates for Microsoft .NET core and ASP.NET (DoS) (July 2018)

Synopsis

The Microsoft ASP.NET Core installations on the remote host contain vulnerable packages.

Description

The Microsoft ASP.NET Core installations on the remote host are missing a security update. It is, therefore, affected by the following vulnerability :
- A security feature bypass vulnerability exists when Microsoft .NET Framework components do not correctly validate certificates.
An attacker could present expired certificates when challenged. The security update addresses the vulnerability by ensuring that .NET Framework components correctly validate certificates. (CVE-2018-8356)

See Also

http://www.nessus.org/u?3e10f501

https://github.com/aspnet/Announcements/issues/311

Solution

Update ASP.NET Core, remove vulnerable packages and refer to vendor advisory.

Risk Factor

Low

Vulnerability Priority Rating (VPR)

3.6

CVSS v3.0 Base Score

5.5 (AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N)

CVSS v3.0 Temporal Score

4.8 (E:U/RL:O/RC:C)

CVSS Base Score

2.1 (AV:L/AC:L/Au:N/C:N/I:P/A:N)

CVSS Temporal Score

1.6 (E:U/RL:OF/RC:C)

References

CVE	CVE-2018-8356

BID	104664
XREF	MSKB:4339279
XREF	MSFT:MS18-4339279

Plugin Information:

Publication date: 2018/07/13, Modification date: 2019/11/04

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
  Path              : C:\Program Files\dotnet\store\x64\netcoreapp2.0
  Installed version : 2.0.13103.0

  Package           : Microsoft.AspNetCore.Server.Kestrel.Core
  Path              : C:\Program Files\dotnet\store
\x64\netcoreapp2.0\microsoft.aspnetcore.server.kestrel.core\2.0.0\lib
\netstandard2.0\Microsoft.AspNetCore.Server.Kestrel.Core.dll
  Installed version : 2.0.0.17205
  Fixed version     : 2.0.4

  Package           : Microsoft.AspNetCore.Server.Kestrel.Core
  Path              : C:\Program Files\dotnet\store
\x64\netcoreapp2.0\microsoft.aspnetcore.server.kestrel.core\2.0.1\lib
\netstandard2.0\Microsoft.AspNetCore.Server.Kestrel.Core.dll
  Installed version : 2.0.1.17303
  Fixed version     : 2.0.4

  Package           : Microsoft.AspNetCore.Server.Kestrel.Core
  Path              : C:\Program Files\dotnet\store
\x64\netcoreapp2.0\microsoft.aspnetcore.server.kestrel.core\2.0.2\lib
\netstandard2.0\Microsoft.AspNetCore.Server.Kestrel.Core.dll
  Installed version : 2.0.2.18051
  Fixed version     : 2.0.4

  Package           : Microsoft.AspNetCore.Server.Kestrel.Core
  Path              : C:\Program Files\dotnet\store
\x64\netcoreapp2.0\microsoft.aspnetcore.server.kestrel.core\2.0.3\lib
\netstandard2.0\Microsoft.AspNetCore.Server.Kestrel.Core.dll
  Installed version : 2.0.3.18114
  Fixed version     : 2.0.4
```

44401 - Microsoft Windows SMB Service Config Enumeration

Synopsis

It was possible to enumerate configuration parameters of remote services.

Description

Nessus was able to obtain, via the SMB protocol, the launch parameters of each active service on the remote host (executable path, logon type, etc.).

Solution

Ensure that each service is configured properly.

Risk Factor

None

Plugin Information:

Publication date: 2010/02/05, Modification date: 2019/11/22

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
The following services are set to start automatically :

  AGMService startup parameters :
    Display name : Adobe Genuine Monitor Service
    Service name : AGMService
    Log on as : LocalSystem
    Executable path : "C:\Program Files (x86)\Common Files\Adobe\AdobeGCClient\AGMService.exe"
```

```
AGSService startup parameters :
  Display name : Adobe Genuine Software Integrity Service
  Service name : AGSService
  Log on as : LocalSystem
  Executable path : "C:\Program Files (x86)\Common Files\Adobe\AdobeGCClient\AGSService.exe"

AdobeARMservice startup parameters :
  Display name : Adobe Acrobat Update Service
  Service name : AdobeARMservice
  Log on as : LocalSystem
  Executable path : "C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe"

AppHostSvc startup parameters :
  Display name : Application Host Helper Service
  Service name : AppHostSvc
  Log on as : localSystem
  Executable path : C:\WINDOWS\system32\svchost.exe -k apphost

AudioEndpointBuilder startup parameters :
  Display name : Windows Audio Endpoint Builder
  Service name : AudioEndpointBuilder
  Log on as : LocalSystem
  Executable path : C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted -p

Audiosrv startup parameters :
  Display name : Windows Audio
  Service name : Audiosrv
  Log on as : NT AUTHORITY\LocalService
  Executable path : C:\WINDOWS\System32\svchost.exe -k LocalServiceNetworkRestricted -p
  Dependencies : AudioEndpointBuilder/RpcSs/

BFE startup parameters :
  Display name : Base Filtering Engine
  Service name : BFE
  Log on as : NT AUTHORITY\LocalService
  Executable path : C:\WINDOWS\system32\svchost.exe -k LocalServiceNoNetworkFirewall -p
  Dependencies : RpcSs/

BITS startup parameters :
  Display name : Background Intelligent Transfer Service
  Service name : BITS
  Log on as : LocalSystem
  Executable path : C:\WINDOWS\System32\svchost.exe -k netsvcs -p
  Dependencies : RpcSs/

BrokerInfrastructure startup parameters :
  [...]
```

92370 - Microsoft Windows ARP Table

Synopsis

Nessus was able to collect and report ARP table information from the remote host.

Description

Nessus was able to collect ARP table information from the remote Windows host and generate a report as a CSV attachment.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2020/06/23

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
10.0.0.1 : 44-f4-77-ba-5a-41
10.0.0.20 : 00-50-56-ac-20-54
10.0.0.21 : 00-50-56-ac-13-54
10.0.0.22 : 00-50-56-ac-20-b6
```

```
10.0.0.23 : 00-50-56-ac-72-6f
10.0.0.24 : 00-50-56-9a-72-98
10.0.0.44 : 00-50-56-9a-a4-d3
10.0.0.54 : 00-50-56-94-24-84
10.0.0.60 : 00-50-56-94-69-66
10.0.0.61 : 00-50-56-ac-65-8a
10.0.0.70 : 00-50-56-94-67-6b
10.0.0.83 : 00-50-56-94-7d-86
10.0.0.85 : 00-50-56-94-24-84
10.0.0.88 : 00-50-56-94-24-84
10.0.0.89 : 00-50-56-94-24-84
10.0.0.223 : 00-50-56-94-44-20
10.0.1.6 : 00-50-56-94-3d-25
10.0.1.24 : 00-50-56-a6-c2-ba
10.0.1.25 : 00-50-56-94-5d-6e
10.0.1.54 : 00-50-56-a6-c4-be
10.0.1.55 : 00-50-56-ac-21-2d
10.0.1.62 : 00-50-56-ac-09-09
10.0.1.103 : 00-50-56-9a-d1-3f
10.0.1.115 : 00-50-56-a6-6a-77
10.0.1.140 : 00-50-56-ac-74-67
10.0.1.141 : 00-50-56-ac-74-67
10.0.1.150 : 00-50-56-ac-33-f6
10.0.1.217 : 00-50-56-ac-3b-5a
10.0.1.220 : 00-50-56-ac-6e-e8
10.0.1.239 : 00-50-56-9a-f3-e5
10.0.1.254 : 54-75-d0-d5-77-a8
10.0.40.1 : 00-50-56-9a-5c-dc
10.0.40.3 : 00-50-56-9a-22-7a
10.0.40.6 : 00-50-56-9a-f8-6d
10.0.50.3 : 00-50-56-9a-f7-c8
10.0.77.43 : a0-36-9f-27-d7-04
10.0.100.3 : 00-50-56-a6-79-f5
10.0.100.5 : 00-50-56-9a-03-68
10.0.101.131 : 00-50-56-a6-84-33
10.0.103.102 : 00-50-56-9a-66-c6
10.0.103.104 : 00-50-56-9a-26-6c
10.0.103.105 : 00-50-56-9a-8b-12
10.0.103.106 : 00-50-56-9a-68-61
10.0.103.108 : 00-50-56-9a-91-36
10.0.103.110 : 00-50-56-9a-34-90
10.0.103.112 : 00-50-56-9a-f9-bd
10.0.103.114 : 00-50-56-9a-89-b1
10.0.103.121 : 00-50-56-9a-e7-e1
10.0.103.124 : 00-50-56-9a-57-33
10.0.103.126 : 00-50-56-9a-d3-59
10.0.103.127 : 00-50-56-9a-2d-e4
10.0.255.255 : ff-ff-ff-ff-ff-ff
224.0.0.18 : 01-00-5e-00-00-12
224.0.0.22 : 01-00-5e-00-00-16
224.0.0.251 : 01-00-5e-00-00-fb
224.0.0.252 : 01-00-5e-00-00-fc
239.255.255.250 : 01-00-5e-7f-ff-fa

Extended ARP table information attached.
```

85736 - Windows Store Application Enumeration

Synopsis

It is possible to obtain the list of applications installed from the Windows Store.

Description

This plugin connects to the remote Windows host with the supplied credentials and uses WMI and Powershell to enumerate applications installed on the host from the Windows Store.

See Also

https://www.microsoft.com/en-us/store/apps

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2015/09/02, Modification date: 2020/06/23

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
-Microsoft.NET.Native.Runtime.1.3
    Version : 1.3.23901.0
    Architecture : X86
    Publisher : CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US

-Microsoft.NET.Native.Runtime.1.3
    Version : 1.3.23901.0
    Architecture : X64
    Publisher : CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US

-Microsoft.Appconnector
    Version : 1.3.3.0
    Architecture : Neutral
    Publisher : CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US

-Microsoft.ConnectivityStore
    Version : 1.1604.4.0
    Architecture : X64
    Publisher : CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US

-Microsoft.NET.Native.Framework.1.0
    Version : 1.0.22929.0
    Architecture : X64
    Publisher : CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US

-Microsoft.NET.Native.Framework.1.0
    Version : 1.0.22929.0
    Architecture : X86
    Publisher : CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US

-Microsoft.NET.Native.Framework.1.1
    Version : 1.0.23115.0
    Architecture : X64
    Publisher : CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US

-Microsoft.NET.Native.Framework.1.1
    Version : 1.0.23115.0
    Architecture : X86
    Publisher : CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US

-Microsoft.NET.Native.Framework.1.2
    Version : 1.2.23231.0
    Architecture : X64
    Publisher : CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US

-Microsoft.NET.Native.Runtime.1.0
    Version : 1.0.22929.0
    Architecture : X64
    Publisher : CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US

-Microsoft.NET.Native.Runtime.1.0
    Version : 1.0.22929.0
    Architecture : X86
    Publisher : CN=Microsoft Corporation, O=Microsoft Corporation, [...]
```

58181 - Windows DNS Server Enumeration

Synopsis

Nessus enumerated the DNS servers being used by the remote Windows host.

Description

Nessus was able to enumerate the DNS servers configured on the remote Windows host by looking in the registry.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2012/03/01, Modification date: 2020/01/22

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Nessus enumerated DNS servers for the following interfaces :

Interface: {97afe548-6ac7-486e-b657-0600d22b7a1c}
Network Connection : Ethernet0 2
NameServer: 10.0.0.20,10.0.0.21
```

10400 - Microsoft Windows SMB Registry Remotely Accessible

Synopsis

Access the remote Windows Registry.

Description

It was possible to access the remote Windows Registry using the login / password combination used for the Windows local checks (SMB tests).

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/05/09, Modification date: 2020/01/22

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :
- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- Whether credentialed or third-party patch management checks are possible.
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/08/26, Modification date: 2020/06/12

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
Information about this scan :

Nessus version : 7.7.0
Plugin feed version : 202006262314
Scanner edition used : Nessus
Scan type : Windows Agent
```

```
Scan policy used : Basic Agent Scan
Scanner IP : 127.0.0.1
Thorough tests : yes
Experimental tests : no
Paranoia level : 0
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : yes
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 5
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2020/6/29 14:31 GMT Standard Time
Scan duration : 5873 sec
```

97086 - Server Message Block (SMB) Protocol Version 1 Enabled

Synopsis

The remote Windows host supports the SMBv1 protocol.

Description

The remote Windows host supports Server Message Block Protocol version 1 (SMBv1). Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions. Additionally, the Shadow Brokers group reportedly has an exploit that affects SMB; however, it is unknown if the exploit affects SMBv1 or another version. In response to this, US-CERT recommends that users disable SMBv1 per SMB best practices to mitigate these potential issues.

See Also

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

https://support.microsoft.com/en-us/help/2696547/how-to-detect-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and

http://www.nessus.org/u?8dcab5e4

http://www.nessus.org/u?234f8ef8

http://www.nessus.org/u?4c7e0cf3

Solution

Disable SMBv1 according to the vendor instructions in Microsoft KB2696547. Additionally, block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk Factor

None

Plugin Information:

Publication date: 2017/02/09, Modification date: 2020/06/12

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
SMBv1 server is enabled :
  - HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\SMB1 : NULL or missing
SMB1protocol feature is enabled based on the following key :
  - HKLM\SYSTEM\CurrentControlSet\Services\srv
SMBv1 client is enabled :
  - HKLM\SYSTEM\CurrentControlSet\Services\mrxsmb10\Start : 2
```

88700 - Microsoft Visual Studio Installed

Synopsis

The remote Windows host has an integrated development environment installed.

Description

Microsoft Visual Studio, an integrated development environment application, is installed on the remote Windows host.

See Also

https://visualstudio.microsoft.com/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/02/11, Modification date: 2020/06/23

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Nessus detected 2 installs of Microsoft Visual Studio:

  Path    : C:\Program Files (x86)\Microsoft Visual Studio 12.0\
  Version : 12.0.40629.0
  Product : 2013

  Path    : C:\Program Files (x86)\Microsoft Visual Studio\2017\Community\Common7\IDE\devenv.exe
  Version : 15.9.28307.1093
  Product : 2017
```

92430 - Registry Editor Last Accessed

Synopsis

Nessus was able to find the last key accessed by the Registry Editor when it was closed on the remote host.

Description

Nessus was able to find evidence of the last key that was opened when the Registry Editor was closed for each user.

See Also

https://support.microsoft.com/en-us/help/244004

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2018/11/15

Ports

vda-it-ts (TCP/0) Vulnerability State: Resurfaced

```
EDENBROWN.UK\t.styles
  - Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome
```

136969 - Microsoft Edge Chromium Installed

Synopsis

Microsoft Edge (Chromium-based) is installed on the remote host.

Description

Microsoft Edge (Chromium-based), a Chromium-based web browser, is installed on the remote host.

See Also

https://www.microsoft.com/en-us/edge

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2020/05/29, Modification date: 2020/06/23

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Path    : C:\Program Files (x86)\Microsoft\Edge\Application
Version : 83.0.478.56
```

131186 - Microsoft Visual Studio Integrated Shell Installed

Synopsis

The remote Windows host has one or more applications built on top of Microsoft Visual Studio Integrated Shell.

Description

Microsoft Visual Studio Integrated Shell, a base IDE to build tools and applications on top of Visual Studio, is installed on the remote Windows host.

See Also

https://docs.microsoft.com/en-us/visualstudio/extensibility/visual-studio-shell-integrated?view=vs-2015

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2019/11/22, Modification date: 2020/06/23

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Path    : C:\Program Files (x86)\Microsoft Visual Studio 11.0\
Version : 11.0.61219.0
Product : 2012
```

20811 - Microsoft Windows Installed Software Enumeration (credentialed check)

Synopsis

It is possible to enumerate installed software.

Description

This plugin lists software potentially installed on the remote host by crawling the registry entries in :
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall HKLM\SOFTWARE\Microsoft\Updates
Note that these entries do not necessarily mean the applications are actually installed on the remote host - they may have been left behind by uninstallers, or the associated files may have been manually removed.

Solution

Remove any applications that are not compliant with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Publication date: 2006/01/26, Modification date: 2020/04/02

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
The following software are installed on the remote host :

Adobe Flash Player 32 NPAPI  [version 32.0.0.387]
Core FTP LE (x64)
DBeaver 6.0.5  [version 6.0.5]
FileZilla Client 3.48.1  [version 3.48.1]
HitmanPro.Alert 3 (managed by Sophos)  [version 3.7.15.446]
```

```
Service Pack 1 for SQL Server 2012 (KB2674319)  [version 11.1.3000.0]  [installed on 2014/10/08]
GDR 3128 for SQL Server 2012 (KB2793634)  [version 11.1.3128.0]  [installed on 2014/10/09]
Hotfix 2430 for SQL Server 2014 (KB2999197)  [version 12.0.2430.0]  [installed on 2017/02/16]
Service Pack 1 for SQL Server 2014 (KB3058865) (64-bit)  [version 12.1.4100.1]  [installed on
 2016/04/25]
Hotfix 2569 for SQL Server 2014 (KB3158271)  [version 12.0.2569.0]  [installed on 2018/11/09]
Hotfix 4459 for SQL Server 2014 (KB3162659) (64-bit)  [version 12.1.4459.0]  [installed on
 2016/07/21]
Hotfix 4522 for SQL Server 2014 (KB4019099) (64-bit)  [version 12.1.4522.0]  [installed on
 2018/11/09]
LastPass (uninstall only)
Magic ISO Maker v5.5 (build 0281)
Microsoft Azure Compute Emulator - v2.9.6  [version 2.9.8899.26]  [installed on 12/05/2020]
Microsoft Azure Storage Emulator - v5.7  [version 5.7.18218.1723]
Microsoft Edge  [version 83.0.478.56]  [installed on 2020/06/26]
Microsoft Edge Update  [version 1.3.129.31]
Microsoft Help Viewer 1.1  [version 1.1.40219]
Microsoft Help Viewer 2.0  [version 2.0.50727]
Microsoft Help Viewer 2.1  [version 2.1.21005]
Microsoft Help Viewer 2.2  [version 2.2.25420]
Microsoft Report Viewer Redistributable 2008 SP1
Microsoft SQL Server 2012
Microsoft SQL Server 2014 (64-bit)
Microsoft SQL Server 2016
Microsoft SQL Server 2017
Microsoft Team Foundation Server 2010 Object Model (VSLS) - ENU  [version 10.0.40219]
Microsoft Visual J# 2.0 Redistributable Package - SE (x64)
Microsoft Visual Studio 2010 Tools for Office Runtime (x64)  [version 10.0.50903]
Mozilla Firefox 77.0.1 (x64 en-US)  [version 77.0.1]
Mozilla Firefox 77.0.1 (x86 en-US)  [version 77.0.1]
Mozilla Maintenance Service  [version 77.0.1]
Notepad++ (32-bit x86)  [version [...]
```

65791 - Microsoft Windows Portable Devices

Synopsis

It is possible to get a list of portable devices that may have been connected to the remote system in the past.

Description

By connecting to the remote host with the supplied credentials, this plugin enumerates portable devices that have been connected to the remote host in the past.

See Also

http://www.nessus.org/u?af102b66

Solution

Make sure that use of the portable devices agrees with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Publication date: 2013/04/03, Modification date: 2019/11/22

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
  Friendly name : J:\
  Device        : SWD#WPDBUSENUM#_??
_USBSTOR#DISK&VEN_SANDISK&PROD_U3_CRUZER_MICRO&REV_2.18#00001855E86196B6&0#{53F56307-
B6BF-11D0-94F2-00A0C91EFB8B}

  Friendly name : DATA
  Device        : SWD#WPDBUSENUM#{93EAAA6B-1746-11EA-9D5C-005056A64957}#0000000000100000

  Friendly name : USB2
  Device        : WPDBUSENUMROOT#UMB#2&37C186B&0&STORAGE#VOLUME#_??
_USBSTOR#DISK&VEN_&PROD_USB_DISK_2.0&REV_PMAP#070146A2F5196C91&0#

  Friendly name : G:\
  Device        : WPDBUSENUMROOT#UMB#2&37C186B&0&STORAGE#VOLUME#_??
_USBSTOR#DISK&VEN_GENERIC&PROD_FLASH_DISK&REV_8.07#535D8EAA&0#
```

```
  Friendly name : HP v150w
  Device        : WPDBUSENUMROOT#UMB#2&37C186B&0&STORAGE#VOLUME#_??
_USBSTOR#DISK&VEN_HP&PROD_V150W&REV_1100#AE52HE05000000001&0#

  Friendly name : INTENSO
  Device        : WPDBUSENUMROOT#UMB#2&37C186B&0&STORAGE#VOLUME#_??
_USBSTOR#DISK&VEN_INTENSO&PROD_RAINBOW_LINE&REV_#12032800077627&0#

  Friendly name : G:\
  Device        : WPDBUSENUMROOT#UMB#2&37C186B&0&STORAGE#VOLUME#_??
_USBSTOR#DISK&VEN_KINGSTON&PROD_DATATRAVELER_2.0&REV_PMAP#5B8802000146&0#

  Friendly name : L:\
  Device        : WPDBUSENUMROOT#UMB#2&37C186B&0&STORAGE#VOLUME#_??
_USBSTOR#DISK&VEN_SANDISK&PROD_U3_CRUZER_MICRO&REV_2.18#00001855E86196B6&0#

  Friendly name : STORE N GO
  Device        : WPDBUSENUMROOT#UMB#2&37C186B&0&STORAGE#VOLUME#_??
_USBSTOR#DISK&VEN_VERBATIM&PROD_STORE_N_GO&REV_5.00#079B1809EFF7A71E&0#
```

63620 - Windows Product Key Retrieval

Synopsis

This plugin retrieves the Windows Product key of the remote Windows host.

Description

Using the supplied credentials, Nessus was able to obtain the retrieve the Windows host's partial product key'.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/01/18, Modification date: 2013/01/18

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
  Product key : XXXXX-XXXXX-XXXXX-XXXXX-WTYPF

Note that all but the final portion of the key has been obfuscated.
```

55472 - Device Hostname

Synopsis

It was possible to determine the remote system hostname.

Description

This plugin reports a device's hostname collected via SSH or WMI.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/06/30, Modification date: 2020/06/23

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
  Hostname : VDA-IT-TS
    VDA-IT-TS (agent)
```

58290 - Evernote Detection (Windows)

Synopsis

A cloud-based note taking application is installed on the remote host.

Description

Evernote is installed on this host. It is a cloud-based suite of software for note taking and archiving.

See Also

http://www.evernote.com/evernote/

Solution

Make sure that use of this program agrees with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Publication date: 2012/03/08, Modification date: 2019/11/22

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Path    : C:\Program Files (x86)\Evernote\Evernote
Version : 6.25.1.9091
```

72482 - Windows Display Driver Enumeration

Synopsis

Nessus was able to enumerate one or more of the display drivers on the remote host.

Description

Nessus was able to enumerate one or more of the display drivers on the remote host via WMI.

See Also

http://www.nessus.org/u?b6e87533

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2014/02/06, Modification date: 2020/06/23

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
Device Name         : VNC Mirror Driver
Driver File Version : 1.8.0.0
Driver Date         : 03/14/2008

Device Name         : Microsoft Remote Display Adapter
Driver File Version : 10.0.18362.693
Driver Date         : 06/21/2006

Device Name         : VMware SVGA 3D
Driver File Version : 8.16.1.24
Driver Date         : 02/05/2019
Video Processor     : VMware Virtual SVGA 3D Graphics Adapter
```

99364 - Microsoft .NET Security Rollup Enumeration

Synopsis

This plugin enumerates installed Microsoft .NET security rollups.

Description

Nessus was able to enumerate the Microsoft .NET security rollups installed on the remote Windows host.

See Also

http://www.nessus.org/u?662e30c9

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2017/04/14, Modification date: 2020/05/13

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
  .NET version                  : 3.5
  Latest effective update level : 05_2020
  File checked                  : C:\WINDOWS\winsxs\*system.runtime.serialization_b77a5c561934e089*
\system.runtime.serialization.dll
  File version                  : 3.0.4506.9149
  Associated KB                 : 4552931


  .NET version                  : 4.8
  Latest effective update level : 05_2020
  File checked                  : C:\WINDOWS\Microsoft.NET\Framework
\v4.0.30319\system.runtime.serialization.dll
  File version                  : 4.8.4180.0
  Associated KB                 : 4552931
```

105793 - VMware Tools Detection

Synopsis

A virtual machine management application is installed on the remote host.

Description

VMware Tools, a suite of utilities that enhances the performance of the virtual machines guest operating system is installed on the remote Windows host.

See Also

https://kb.vmware.com/s/article/340

http://www.nessus.org/u?7d54c30a

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2018/01/13, Modification date: 2020/06/23

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
  Path    : C:\Program Files\VMware\VMware Tools\
  Version : 10.3.10.10540
```

60119 - Microsoft Windows SMB Share Permissions Enumeration

Synopsis

It was possible to enumerate the permissions of remote network shares.

Description

By using the supplied credentials, Nessus was able to enumerate the permissions of network shares. User permissions are enumerated for each network share that has a list of access control entries (ACEs).

See Also

https://technet.microsoft.com/en-us/library/bb456988.aspx

https://technet.microsoft.com/en-us/library/cc783530.aspx

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2012/07/25, Modification date: 2019/11/22

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Share path : \\127.0.0.1\2nd floor 222
Local path : RICOH Class Driver,LocalsplOnly
Comment : RICOH Class Driver
[*] Allow ACE for EDEN_MAIN\t.styles: 0x001f01ff
    FILE_GENERIC_READ:         YES
    FILE_GENERIC_WRITE:        YES
    FILE_GENERIC_EXECUTE:      YES
[*] Allow ACE for Everyone: 0x001f01ff
    FILE_GENERIC_READ:         YES
    FILE_GENERIC_WRITE:        YES
    FILE_GENERIC_EXECUTE:      YES
[*] Allow ACE for APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES: 0x001f01ff
    FILE_GENERIC_READ:         YES
    FILE_GENERIC_WRITE:        YES
    FILE_GENERIC_EXECUTE:      YES
[*] Allow ACE for BUILTIN\Administrators: 0x001f01ff
    FILE_GENERIC_READ:         YES
    FILE_GENERIC_WRITE:        YES
    FILE_GENERIC_EXECUTE:      YES

Share path : \\127.0.0.1\print$
Local path : C:\WINDOWS\system32\spool\drivers
Comment : Printer Drivers
[*] Allow ACE for Everyone: 0x001200a9
    FILE_GENERIC_READ:         YES
    FILE_GENERIC_WRITE:        NO
    FILE_GENERIC_EXECUTE:      YES
[*] Allow ACE for BUILTIN\Administrators: 0x001f01ff
    FILE_GENERIC_READ:         YES
    FILE_GENERIC_WRITE:        YES
    FILE_GENERIC_EXECUTE:      YES
```

92367 - Microsoft Windows PowerShell Execution Policy

Synopsis

Nessus was able to collect and report the PowerShell execution policy for the remote host.

Description

Nessus was able to collect and report the PowerShell execution policy for the remote Windows host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2020/06/12

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
HKLM\SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell\ExecutionPolicy : AllSigned
HKLM\SOFTWARE\Wow6432Node\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell\ExecutionPolicy :
 AllSigned
```

93232 - Microsoft Office Compatibility Pack Installed (credentialed check)

Synopsis

A compatibility application is installed on the remote host.

Description

Microsoft Office Compatibility Pack, used to enable older versions of Microsoft Office applications to view and edit files created with newer versions of Microsoft Office applications, is installed on the remote Windows host.

See Also

https://support.microsoft.com/en-us/help/923505

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/08/30, Modification date: 2020/06/12

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Office Compatibility Pack is installed with the following components:

  Component : Excel Converter
  Version   : 16.0.12624.20466
  Path      : C:\Program Files\Microsoft Office\root\Office16\Excelcnv.exe

  Component : Word Converter
  Version   : 16.0.12624.20466
  Path      : C:\Program Files\Microsoft Office\root\Office16\Wordconv.exe

Office Compatibility Pack is installed with the following components:

  Component : Excel Converter
  Version   : 14.0.7248.5000
  Path      : C:\Program Files\Microsoft Office\Office14\Excelcnv.exe

  Component : Word Converter
  Version   : 14.0.4762.1000
  Path      : C:\Program Files\Microsoft Office\Office14\Wordconv.exe
```

77668 - Windows Prefetch Folder

Synopsis

Nessus was able to retrieve the Windows prefetch folder file list.

Description

Nessus was able to retrieve and display the contents of the Windows prefetch folder (%systemroot%\prefetch*). This information shows programs that have run with the prefetch and superfetch mechanisms enabled.

See Also

http://www.nessus.org/u?8242d04f

http://www.nessus.org/u?d6b15983

http://www.forensicswiki.org/wiki/Prefetch

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2014/09/12, Modification date: 2018/11/15

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
 + HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters
rootdirpath :
enableprefetcher : 3
```

```
+ Prefetch file list :
  - \WINDOWS\prefetch\314519-FIREFOX SETUP 77.0.1.E-7EB51C55.pf
  - \WINDOWS\prefetch\7Z.EXE-16F55E58.pf
  - \WINDOWS\prefetch\7ZA.EXE-8846DBDD.pf
  - \WINDOWS\prefetch\7ZG.EXE-0F8C4081.pf
  - \WINDOWS\prefetch\ACRORD32.EXE-ACF2947E.pf
  - \WINDOWS\prefetch\ACRORD32.EXE-D066635E.pf
  - \WINDOWS\prefetch\AGSSERVICE.EXE-002E2A8C.pf
  - \WINDOWS\prefetch\APPLICATIONFRAMEHOST.EXE-CCEEF759.pf
  - \WINDOWS\prefetch\ARP.EXE-2BC38967.pf
  - \WINDOWS\prefetch\ATMGR.EXE-10D6D3AA.pf
  - \WINDOWS\prefetch\AUDIODG.EXE-BDFD3029.pf
  - \WINDOWS\prefetch\AUTELEM.EXE-2CA33471.pf
  - \WINDOWS\prefetch\BACKGROUNDSCANCLIENT.EXE-AA853FC3.pf
  - \WINDOWS\prefetch\BACKGROUNDTASKHOST.EXE-42FBC963.pf
  - \WINDOWS\prefetch\BACKGROUNDTASKHOST.EXE-901440A8.pf
  - \WINDOWS\prefetch\BACKGROUNDTASKHOST.EXE-9898D8ED.pf
  - \WINDOWS\prefetch\BACKGROUNDTASKHOST.EXE-A4F5A8B5.pf
  - \WINDOWS\prefetch\BACKGROUNDTASKHOST.EXE-E877731E.pf
  - \WINDOWS\prefetch\BACKGROUNDTASKHOST.EXE-EA6348AC.pf
  - \WINDOWS\prefetch\BACKGROUNDTASKHOST.EXE-F1750873.pf
  - \WINDOWS\prefetch\CALCULATOR.EXE-8351C79E.pf
  - \WINDOWS\prefetch\CEFSHARP.BROWSERSUBPROCESS.EX-0C34C85B.pf
  - \WINDOWS\prefetch\CEFSHARP.BROWSERSUBPROCESS.EX-0C34C85C.pf
  - \WINDOWS\prefetch\CEFSHARP.BROWSERSUBPROCESS.EX-0C34C85D.pf
  - \WINDOWS\prefetch\CEFSHARP.BROWSERSUBPROCESS.EX-0C34C863.pf
  - \WINDOWS\prefetch\CHROME.EXE-D999B1BA.pf
  - \WINDOWS\prefetch\CHROME.EXE-D999B1BB.pf
  - \WINDOWS\prefetch\CHROME.EXE-D999B1BC.pf
  - \WINDOWS\prefetch\CHROME.EXE-D999B1C1.pf
  - \WINDOWS\prefetch\CHROME.EXE-D999B1C2.pf
  - \WINDOWS\prefetch\CHXSMARTSCREEN.EXE-CD856DA3.pf
  - \WINDOWS\prefetch\CISCOWEBEXSTART.EXE-4617802C.pf
  - \WINDOWS\prefetch\CLEANMGR.EXE-E3C5E89D.pf
  - \WINDOWS\prefetch\CLOUDNOTIFICATIONS.EXE-32AFFBA5.pf
  - \WINDOWS\prefetch\CMD.EXE-4A81B364.pf
  - \WINDOWS\prefetch\CMD.EXE-AC113AA8.pf
  - [...]
```

66517 - Adobe Reader Enabled in Browser (Internet Explorer)

Synopsis

The remote host has Adobe Reader enabled for Internet Explorer.

Description

Adobe Reader is enabled in Internet Explorer.

Solution

Disable Adobe Reader unless it is needed.

Risk Factor

None

Plugin Information:

Publication date: 2013/05/20, Modification date: 2016/06/13

Ports

vda-it-ts (TCP/445) Vulnerability State: Resurfaced

```
Adobe Reader is enabled for the following SIDs :
  S-1-5-21-289213053-1965310637-929701000-34059
  S-1-5-21-289213053-1965310637-929701000-43470

Note that this check may be incomplete as Nessus can only check the
SIDs of logged on users.
```

72367 - Microsoft Internet Explorer Version Detection

Synopsis

Internet Explorer is installed on the remote host.

Description

The remote Windows host contains Internet Explorer, a web browser created by Microsoft.

See Also

https://support.microsoft.com/en-us/help/17621/internet-explorer-downloads

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2014/02/06, Modification date: 2019/11/22

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Version  : 11.900.18362.0
```

92422 - Windows Mapped Network Drives

Synopsis

Nessus was able to enumerate mapped network drives on the remote host.

Description

Nessus was able to generate a report of mapped network drives on the remote Windows host.

See Also

http://www.nessus.org/u?73356601

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc770902(v=ws.11)

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2018/11/15

Ports

vda-it-ts (TCP/0) Vulnerability State: Resurfaced

```
b : \\data01\netwrix$
mrulist : edcba
e : \\data01\marketing
d : \\data01\facilities
c : \\london-coleman\c$
a : \\data01\ISO$


Extended mapped network drive report attached.
```

124175 - Oracle MySQL Connectors Installed (Windows)

Synopsis

One or more connectors for Oracle MySQL are installed on the remote Windows host.

Description

Oracle MySQL connectors, drivers for connecting to MySQL databases, are installed on the remote Windows host.
Note: Thorough tests may be required for an in-depth search of all connectors.

See Also

https://www.mysql.com/products/connector/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2019/04/19, Modification date: 2020/06/23

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Nessus detected 2 installs of MySQL Connector:

  Path    : C:\Program Files (x86)\MySQL\Connector ODBC 5.1\
  Version : 5.1.10
  Product : MySQL Connector/ODBC

  Path    : C:\Program Files\MySQL\Connector ODBC 5.1\
  Version : 5.1.10
  Product : MySQL Connector/ODBC
```

92439 - Explorer Search History

Synopsis

Nessus was able to gather a list of items searched for in the Windows UI.

Description

Nessus was able to gather evidence of cached search results from Windows Explorer searches.

See Also

https://www.4n6k.com/2015/05/forensics-quickie-ntuserdat-analysis.html

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2018/11/15

Ports

vda-it-ts (TCP/0) Vulnerability State: Resurfaced

```
Explorer search history report attached.
```

10456 - Microsoft Windows SMB Service Enumeration

Synopsis

It is possible to enumerate remote services.

Description

This plugin implements the SvcOpenSCManager() and SvcEnumServices() calls to obtain, using the SMB protocol, the list of active and inactive services of the remote host.
An attacker may use this feature to gain better knowledge of the remote host.

Solution

To prevent the listing of the services from being obtained, you should either have tight login restrictions, so that only trusted users can access your host, and/or you should filter incoming traffic to this port.

Risk Factor

None

Plugin Information:

Publication date: 2000/07/03, Modification date: 2019/11/22

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Active Services :
```

```
Adobe Acrobat Update Service [ AdobeARMservice ]
Adobe Genuine Monitor Service [ AGMService ]
Adobe Genuine Software Integrity Service [ AGSService ]
Application Host Helper Service [ AppHostSvc ]
Application Information [ Appinfo ]
Windows Audio Endpoint Builder [ AudioEndpointBuilder ]
Windows Audio [ Audiosrv ]
Base Filtering Engine [ BFE ]
Background Intelligent Transfer Service [ BITS ]
Background Tasks Infrastructure Service [ BrokerInfrastructure ]
Computer Browser [ Browser ]
AVCTP service [ BthAvctpSvc ]
Connected Devices Platform Service [ CDPSvc ]
Certificate Propagation [ CertPropSvc ]
Microsoft Office Click-to-Run Service [ ClickToRunSvc ]
Client License Service (ClipSVC) [ ClipSVC ]
CoreMessaging [ CoreMessagingRegistrar ]
Cryptographic Services [ CryptSvc ]
Offline Files [ CscService ]
DCOM Server Process Launcher [ DcomLaunch ]
Device Association Service [ DeviceAssociationService ]
DHCP Client [ Dhcp ]
Connected User Experiences and Telemetry [ DiagTrack ]
Display Policy Service [ DispBrokerDesktopSvc ]
Display Enhancement Service [ DisplayEnhancementService ]
DNS Client [ Dnscache ]
Diagnostic Policy Service [ DPS ]
Data Sharing Service [ DsSvc ]
Data Usage [ DusmSvc ]
Encrypting File System (EFS) [ EFS ]
Windows Event Log [ EventLog ]
COM+ Event System [ EventSystem ]
Windows Font Cache Service [ FontCache ]
HitmanPro.Alert service [ hmpalertsvc ]
IIS Admin Service [ IISADMIN ]
IKE and AuthIP IPsec Keying Modules [ IKEEXT ]
Microsoft Store Install Service [ InstallService ]
IP Helper [ iphlpsvc ]
Windows Phone IP over USB Transport (IpOverUsbSvc) [ IpOverUsbSvc ]
CNG Key Isolation [ KeyIso ]
Server [ LanmanServer ]
Workstation [ LanmanWorkstation ]
Geolocation Service [ lfsvc ]
Windows License Manager Service [ LicenseManager ]
TCP/IP NetBIOS Helper [ lmhosts ]
Local Session Manager [ LSM ]
ManageEngine Patch Manager Plus - Agent [ ManageEngine Patch Manager Plus - Agent ]
Windows Defender Firewall [ mpssvc ]
Distributed [...]
```

92427 - Microsoft Paint Recent File History

Synopsis

Nessus was able to enumerate files opened in Microsoft Paint on the remote host.

Description

Nessus was able to generate a list of files opened using the Microsoft Paint program.

See Also

https://en.wikipedia.org/wiki/Microsoft_Paint

http://www.nessus.org/u?0887d2d5

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2018/05/23

Ports

vda-it-ts (TCP/0) Vulnerability State: Resurfaced

```
EDENBROWN.UK\t.styles
  - C:\Users\t.styles\OneDrive - nGAGE Specialist Recruitment Limited 1\PowerBI\Retinue\Logos
\NHS_GGC_logo.png
  - C:\Users\t.styles\OneDrive - nGAGE Specialist Recruitment Limited 1\PowerBI\Retinue\Logos\NHS
 Greater Glasgow and Clyde.png
  - C:\Users\t.styles\Pictures\mitie_23516903122.png
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2003/12/09, Modification date: 2020/03/09

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
Remote operating system : Microsoft Windows 10 Enterprise
Confidence level : 100
Method : SMB_OS


The remote host is running Microsoft Windows 10 Enterprise
```

92438 - WordPad History

Synopsis

Nessus was able to gather WordPad opened file history on the remote host.

Description

Nessus was able to generate a report of files opened in WordPad on the remote host.

See Also

https://en.wikipedia.org/wiki/WordPad

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2018/05/23

Ports

vda-it-ts (TCP/0) Vulnerability State: Resurfaced

```
C:\Users\t.styles\Downloads\ian_athol.xml
C:\Users\t.styles\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook
\H0XNN1L3\example_xml_feed_caritas (002).xml
P:\ADCourier\template_cand_resp.csv
C:\Users\t.styles\Downloads\MAT_Jobs_xml.xml

WordPad report attached.
```

92372 - Microsoft Windows NetBIOS over TCP/IP Info

Synopsis

Nessus was able to collect and report NBT information from the remote host.

Description

Nessus was able to collect details for NetBIOS over TCP/IP from the remote Windows host and generate a report as a CSV attachment.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2020/06/23

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
NBT information attached.
```

68879 - Microsoft Lync Installed

Synopsis

A communication application is installed on the remote Windows host.

Description

Microsoft Lync (previously known as Microsoft Office Communications) is installed on the remote host. Microsoft Lync provides communications services such as instant messaging, VoIP, and video conferencing.

See Also

https://products.office.com/en-us/skype-for-business/online-meetings

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/07/14, Modification date: 2019/11/22

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Path    : C:\Program Files\Microsoft Office\root\Office16\
Version : 16.0.12624.20466
Product : Microsoft Lync
```

48763 - Microsoft Windows 'CWDIllegalInDllSearch' Registry Setting

Synopsis

CWDIllegalInDllSearch Settings: Improper settings could allow code execution attacks.

Description

Windows Hosts can be hardened against DLL hijacking attacks by setting the The 'CWDIllegalInDllSearch' registry entry in to one of the following settings:
- 0xFFFFFFFF (Removes the current working directory from the default DLL search order)
- 1 (Blocks a DLL Load from the current working directory if the current working directory is set to a WebDAV folder)
- 2 (Blocks a DLL Load from the current working directory if the current working directory is set to a remote folder)

See Also

http://www.nessus.org/u?0c574c56

http://www.nessus.org/u?5234ef0c

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/08/26, Modification date: 2019/12/20

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Name  : SYSTEM\CurrentControlSet\Control\Session Manager\CWDIllegalInDllSearch
Value : Registry Key Empty or Missing
```

65743 - Oracle Java JRE Enabled (Internet Explorer)

Synopsis

The remote host has Oracle Java JRE enabled for Internet Explorer.

Description

Oracle Java JRE is enabled in Internet Explorer.

See Also

https://support.microsoft.com/en-us/help/2751647/how-to-disable-the-java-web-plug-in-in-internet-explorer

Solution

Apply Microsoft 'Fix it' 50994 unless Java is needed.

Risk Factor

None

Plugin Information:

Publication date: 2013/03/29, Modification date: 2018/11/15

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Java is enabled for the following ActiveX controls and SIDs :
ActiveX CLSIDs :
  {8AD9C840-044E-11D1-B3E9-00805F499D93}
  {CAFEEFAC-0017-0000-FFFF-ABCDEFFEDCBA}
  {CAFEEFAC-0017-0001-FFFF-ABCDEFFEDCBA}
  {CAFEEFAC-0017-0002-FFFF-ABCDEFFEDCBA}
  {CAFEEFAC-0017-0003-FFFF-ABCDEFFEDCBA}
  {CAFEEFAC-0017-0004-FFFF-ABCDEFFEDCBA}
  {CAFEEFAC-0017-0005-FFFF-ABCDEFFEDCBA}
  {CAFEEFAC-0017-0006-FFFF-ABCDEFFEDCBA}
  {CAFEEFAC-FFFF-FFFF-FFFF-ABCDEFFEDCBA}

User SIDs :
  S-1-5-21-289213053-1965310637-929701000-34059

Note that this check may be incomplete as Nessus can only check the
SIDs of logged on users.
```

58452 - Microsoft Windows Startup Software Enumeration

Synopsis

It is possible to enumerate startup software.

Description

This plugin lists software that is configured to run on system startup by crawling the registry entries in :
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersi on\Run

Solution

Review the list of applications and remove any that are not compliant with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Publication date: 2012/03/23, Modification date: 2019/11/22

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
The following startup item was found :

  AdobeGCInvoker-1.0 - C:\Program Files (x86)\Common Files\Adobe\AdobeGCClient
\AGCInvokerUtility.exe
  BCSSync - C:\Program Files\Microsoft Office\Office14\BCSSync.exe
  MSD.Desktop - C:\Program Files\Mimecast\Mimecast Windows Service\msddsk.exe
  SecurityHealth - %windir%\system32\SecurityHealthSystray.exe
  Sophos UI.exe - C:\Program Files\Sophos\Sophos UI\Sophos UI.exe
  TeamsMachineInstaller - %ProgramFiles%\Teams Installer\Teams.exe --checkInstall --source=PROPLUS
  VMware User Process - C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
```

102083 - Microsoft Access Installed (credentialed check)

Synopsis

A database application is installed on the remote Windows host.

Description

Microsoft Access, a database management system, is installed on the remote Windows host.

See Also

http://www.nessus.org/u?10ea70b7

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2017/07/31, Modification date: 2020/06/12

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Nessus detected 2 installs of Microsoft Access:

  Path         : C:\Program Files\Microsoft Office\Office14\MsAccess.exe
  Version      : 14.0.7248.5000
  Product      : 2010
  Service Pack : SP2

  Path         : C:\Program Files\Microsoft Office\root\Office16\MsAccess.exe
  Version      : 16.0.12624.20466
  Product      : 2016
  Service Pack : SP0
```

96533 - Chrome Browser Extension Enumeration

Synopsis

One or more Chrome browser extensions are installed on the remote host.

Description

Nessus was able to enumerate Chrome browser extensions installed on the remote host.

See Also

https://chrome.google.com/webstore/category/extensions

Solution

Make sure that the use and configuration of these extensions comply with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Publication date: 2017/01/16, Modification date: 2020/06/23

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
User : Tim
|- Browser : Chrome
  |- Add-on information :

    Name        : Google Docs
    Description : Create and edit documents
    Version     : 0.5
    Path        : C:\Users\Tim\AppData\Local\Google\Chrome\User Data\Default\Extensions
\aohghmighlieiainnegkcijnfilokake\0.5_0

    Name        : Google Drive
    Description : Google Drive: create, share and keep all your stuff in one place.
    Version     : 6.3
    Update Date : Jan.  6, 2014 at 21:09:47 GMT
    Path        : C:\Users\Tim\AppData\Local\Google\Chrome\User Data\Default\Extensions
\apdfllckaahabafndbhieahigkjlhalf\6.3_0

    Name        : YouTube
    Description : The world's most popular online video community.
    Version     : 4.2.6
    Update Date : Jan.  6, 2014 at 21:09:49 GMT
    Path        : C:\Users\Tim\AppData\Local\Google\Chrome\User Data\Default\Extensions
\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6_0

    Name        : Google Search
    Description : The fastest way to search the web.
    Version     : 0.0.0.20
    Update Date : Jan.  6, 2014 at 21:09:47 GMT
    Path        : C:\Users\Tim\AppData\Local\Google\Chrome\User Data\Default\Extensions
\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20_0

    Name        : AdBlock
    Description : The most popular Chrome extension, with over 15 million users!  Blocks ads all
 over the web.
    Version     : 2.6.16
    Path        : C:\Users\Tim\AppData\Local\Google\Chrome\User Data\Default\Extensions
\gighmmpiobklfepjocnamgkkbiglidom\2.6.16_0

    Name        : Clearly
    Description : Clearly makes blog posts, articles and webpages clean and easy to read. Save
 them to Evernote to read anywhere.
    Version     : 9.3374.689.453
    Path        : C:\Users\Tim\AppData\Local\Google\Chrome\User Data\Default\Extensions
\iooicodkiihhpojmmeghjclgihfjdjhj\9.3374.689.453_0

    Name        : Google Wallet
    Description : Google Wallet for digital goods
    Version     : 0.0.6.0
    Path        : C:\Users\Tim\AppData\Local\Google\Chrome\User Data\Default\Extensions
\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.0_0

 [...]
```

108712 - Microsoft .NET Core SDK for Windows

Synopsis

.NET Core SDK is installed on the remote Windows host.

Description

.NET Core SDK, a managed software framework, is installed on the remote Windows host.

See Also

https://dotnet.github.io/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2018/03/29, Modification date: 2020/06/23

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Nessus detected 3 installs of .NET Core SDK Windows:

  Path    : C:\\program files\dotnet\\sdk\2.1.202
  Version : 2.1.202.0

  Path    : C:\\program files\dotnet\\sdk\2.1.402
  Version : 2.1.402.0

  Path    : C:\\program files\dotnet\\sdk\2.1.513
  Version : 2.1.513.0
```

42399 - Microsoft Silverlight Detection

Synopsis

The remote host has Microsoft Silverlight installed.

Description

A version of Microsoft's Silverlight is installed on this host.
Microsoft Silverlight is a web application framework that provides functionalities similar to those in Adobe Flash, integrating multimedia, graphics, animations and interactivity into a single runtime environment.

See Also

http://silverlight.net/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/11/05, Modification date: 2019/11/22

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
  Path    : c:\Program Files\Microsoft Silverlight\5.1.50918.0
  Version : 5.1.50918.0
```

118238 - JAR File Detection for Windows

Synopsis

Detected JAR files on the host.

Description

The host contains JAR files, Java Archive files.
Note that this plugin only detects JAR files in commonly used installation directories or a user specified search path.

See Also

https://docs.oracle.com/javase/7/docs/technotes/guides/jar/jar.html

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2018/10/22, Modification date: 2020/06/23

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
 JAR files found: 7263
 - C:\Documents and Settings\All Users\Microsoft\AndroidSDK\25\extras\android\m2repository\com
\android\support\gridlayout-v7\23.2.0\gridlayout-v7-23.2.0-javadoc.jar
 - C:\Program Files (x86)\Java\jdk1.8.0_181\lib\missioncontrol\plugins
\com.jrockit.mc.greychart.ui_5.5.2.174165.jar
 - C:\Users\All Users\Microsoft\AndroidSDK\25\extras\android\m2repository\com\android\support
\support-v4\23.3.0\support-v4-23.3.0-sources.jar
 - C:\ProgramData\Microsoft\AndroidSDK\25\extras\android\m2repository\com\android\support\support-
annotations\24.1.0\support-annotations-24.1.0-sources.jar
 - C:\Program Files\DBeaver\plugins\org.jkiss.dbeaver.ui.navigator_1.0.9.201905192012.jar
 - C:\Program Files\DBeaver\plugins\org.jkiss.dbeaver.ext.generic.ui_1.0.0.201905192012.jar
 - C:\Documents and Settings\All Users\Microsoft\AndroidSDK\25\tools\lib\monitor-x86\plugins
\com.android.ide.eclipse.traceview_25.2.5.3567187.jar
 - C:\Users\All Users\Microsoft\AndroidSDK\25\extras\android\m2repository\com\android\support
\palette-v7\23.3.0\palette-v7-23.3.0-sources.jar
 - C:\Documents and Settings\All Users\Microsoft\AndroidSDK\25\extras\android\m2repository\com
\android\support\recommendation\25.1.1\recommendation-25.1.1-sources.jar
 - C:\Documents and Settings\All Users\Microsoft\AndroidSDK\25\tools\lib\monitor-x86_64\plugins
\org.eclipse.equinox.p2.directorywatcher_1.0.300.v20110808-1657.jar
 - C:\Program Files\Java\jdk1.8.0_181\lib\visualvm\visualvm\core\locale\core_visualvm.jar
 - C:\ProgramData\Microsoft\AndroidSDK\25\extras\android\m2repository\com\android\support
\appcompat-v7\24.2.0\appcompat-v7-24.2.0-javadoc.jar
 - C:\Program Files\Java\jdk1.8.0_181\lib\missioncontrol\plugins
\com.jrockit.mc.components.ui_5.5.2.174165.jar
 - C:\ProgramData\Microsoft\AndroidSDK\25\extras\android\m2repository\com\android\support
\gridlayout-v7\24.0.0-alpha2\gridlayout-v7-24.0.0-alpha2-javadoc.jar
 - C:\Documents and Settings\All [...]
```

92371 - Microsoft Windows DNS Cache

Synopsis

Nessus was able to collect and report DNS cache information from the remote host.

Description

Nessus was able to collect details of the DNS cache from the remote Windows host and generate a report as a CSV attachment.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2020/06/23

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
21.0.113.10.in-addr.arpa
3.100.10.10.in-addr.arpa
3bdtest.edenbrown.uk
3bdtest.edenbrown.uk
api.mycareerpassport.co.uk
autodiscover.ngagerecruitment.com
az725175.vo.msecnd.net
bam.nr-data.net
bi01
bi01
casarray01.edenbrown.uk
crg.vms365-demo.co.uk
crg.vms365-demo.co.uk
ctsrecruitment.vms365-demo.co.uk
ctsrecruitment.vms365-demo.co.uk
dc02.edenbrown.uk
dc03.edenbrown.uk
eresponserecruitmentltd.vms365-demo.co.uk
eresponserecruitmentltd.vms365-demo.co.uk
fawkes.vms365-demo.co.uk
fawkes.vms365-demo.co.uk
haysspecialistrecruitmentltd.vms365-demo.co.uk
haysspecialistrecruitmentltd.vms365-demo.co.uk
humanerecruitment.vms365-demo.co.uk
```

```
    humanerecruitment.vms365-demo.co.uk
    ict.infinity-tracking.net
    mail.ngagerecruitment.com
    meetme.i-resource.co.uk
    meetme.i-resource.co.uk
    ngage-it.vssps.visualstudio.com
    ngagerecruitment.com
    nurseplusandcareplus.vms365-demo.co.uk
    nurseplusandcareplus.vms365-demo.co.uk
    peopletoday.vssps.visualstudio.com
    precedo.vms365-demo.co.uk
    precedo.vms365-demo.co.uk
    resourcinggroup.vms365-demo.co.uk
    resourcinggroup.vms365-demo.co.uk
    rg.vms365-demo.co.uk
    rg.vms365-demo.co.uk
    rgmsp.vms365-demo.co.uk
    rgmsp.vms365-demo.co.uk
    s1849907385.t.eloqua.com
    sec-tws-prod-vip.webex.com
    servicecaresolutions.vms365-demo.co.uk
    servicecaresolutions.vms365-demo.co.uk
    superuser.com
    vmas01.i-resource.co.uk
    vmas01.i-resource.co.uk
    www.evernote.com
    www.ngagerecruitment.com
    www.recruitment-software.net

DNS cache information attached.
```

92361 - Microsoft Office Macros Configuration

Synopsis

Nessus was able to collect and report Office macro configuration data for active accounts on the remote host.

Description

Nessus was able to collect Office macro configuration information for active accounts on the remote Windows host and generate a report as a CSV attachment.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2018/05/16

Ports

vda-it-ts (TCP/0) Vulnerability State: Resurfaced

```
Office macros information attached.
```

92368 - Microsoft Windows Scripting Host Settings

Synopsis

Nessus was able to collect and report the Windows scripting host settings from the remote host.

Description

Nessus was able to collect system and user level Windows scripting host settings from the remote Windows host and generate a report as a CSV attachment.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2018/05/23

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
HKLM\SOFTWARE\Microsoft\Windows Script Host\Settings\displaylogo : 1
HKLM\SOFTWARE\Microsoft\Windows Script Host\Settings\usewinsafer : 1
HKLM\SOFTWARE\Microsoft\Windows Script Host\Settings\silentterminate : 0
HKLM\SOFTWARE\Microsoft\Windows Script Host\Settings\activedebugging : 1
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows Script Host\Settings\displaylogo : 1
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows Script Host\Settings\usewinsafer : 1
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows Script Host\Settings\silentterminate : 0
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows Script Host\Settings\activedebugging : 1

Windows scripting host configuration attached.
```

84239 - Debugging Log Report

Synopsis

This plugin gathers the logs written by other plugins and reports them.

Description

Logs generated by other plugins are reported by this plugin. Plugin debugging must be enabled in the policy in order for this plugin to run.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2015/06/17, Modification date: 2020/02/26

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
Plugin debug log(s) have been attached.
```

16193 - Antivirus Software Check

Synopsis

An antivirus application is installed on the remote host.

Description

An antivirus application is installed on the remote host, and its engine and virus definitions are up to date.

See Also

http://www.nessus.org/u?3ed73b52

https://www.tenable.com/blog/auditing-anti-virus-products-with-nessus

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/01/18, Modification date: 2020/05/21

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Sophos :
Sophos Anti-Virus is installed on the remote host :

  Installation path : C:\Program Files (x86)\Sophos\Sophos Anti-Virus
  Product version   : 10.8.6.215
  Engine version    : 3.78.5.2480


Note that Nessus checked for the existence of the following file :
'C:\Program Files (x86)\Sophos\Sophos Anti-Virus\hawke-sn.ide'
```

34096 - BIOS Info (WMI)

Synopsis

The BIOS info could be read.

Description

It is possible to get information about the BIOS via the host's WMI interface.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2008/09/05, Modification date: 2020/06/23

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
  Vendor       : Phoenix Technologies LTD
  Version      : 6.00
  Release date : 20181212000000.000000+000
  UUID         : 421A03EA-B74A-6B25-DC87-98A0204C730C
  Secure boot  : disabled
```

93234 - Microsoft Visio Viewer Installed (credentialed check)

Synopsis

A drawing viewing application is installed on the remote host.

Description

Microsoft Visio Viewer, used to view drawings created in Microsoft Visio, is installed on the remote Windows host.

See Also

http://www.nessus.org/u?d23736d6

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/08/30, Modification date: 2020/06/12

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Nessus detected 3 installs of Microsoft Visio Viewer:

  Path         : C:\Program Files\Microsoft Office\root\Office16\vviewer.dll
  Version      : 16.0.12624.20422
  Product      : 2016
  Service Pack : SP0

  Path         : C:\Program Files (x86)\Microsoft Office\Office14\vviewer.dll
  Version      : 14.0.7163.5000
  Product      : 2010
  Service Pack : SP2

  Path         : C:\Program Files\Microsoft Office\Office14\vviewer.dll
  Version      : 14.0.7163.5000
  Product      : 2010
  Service Pack : SP2
```

28211 - Flash Player Detection

Synopsis

The remote Windows host contains a browser enhancement for displaying multimedia content.

Description

There is at least one instance of Adobe Flash Player installed on the remote Windows host.

See Also

http://www.adobe.com/products/flashplayer/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/11/14, Modification date: 2019/11/22

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Nessus found the following instances of Flash Player installed on the
remote host :

  - ActiveX control (for Internet Explorer) :
    C:\Windows\System32\Macromed\Flash\Flash.ocx, 32.0.0.387
  - Browser Plugin (for Firefox / Netscape / Opera) :
    C:\WINDOWS\system32\Macromed\Flash\NPSWF64_32_0_0_387.dll, 32.0.0.387
```

131725 - Sophos Anti-Virus Installed (Windows)

Synopsis

An antivirus application is installed on the remote Windows host.

Description

Sophos Anti-Virus, a commercial antivirus software package for Windows, is installed on the remote host.

See Also

https://www.sophos.com/en-us.aspx

https://community.sophos.com/kb/en-us/121984

https://community.sophos.com/kb/en-us/120189

https://downloads.sophos.com/downloads/info/latest_IDE.xml

Solution

n/a.

Risk Factor

None

Plugin Information:

Publication date: 2019/12/05, Modification date: 2020/06/26

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
  Path               : C:\Program Files (x86)\Sophos\Sophos Anti-Virus
  Version            : 10.8.6.215
  Cloud Subscription : RECOMMENDED
  Product            : Sophos Anti-Virus
```

70329 - Microsoft Windows Process Information

Synopsis

Use WMI to obtain running process information.

Description

Report details on the running processes on the machine.
This plugin is informative only and could be used for forensic investigation, malware detection, and to confirm that your system processes conform to your system policies.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/10/08, Modification date: 2020/06/23

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
 Process Overview :
SID: Process (PID)
 0 : System Idle Process (0)
 0 : |- System (4)
 0 :    |- Memory Compression (2888)
 0 :    |- smss.exe (412)
 0 : Registry (104)
 2 : Teams.exe (12244)
 2 : |- Teams.exe (11244)
 2 : |- Teams.exe (12404)
 2 : |- Teams.exe (14452)
 2 : |- Teams.exe (27708)
 2 : |- Teams.exe (9392)
 2 : Evernote.exe (144948)
 2 : |- EvernoteSubprocess.exe (131816)
 2 : |- EvernoteSubprocess.exe (163272)
 2 : |- EvernoteTray.exe (254220)
 2 : |- EvernoteSubprocess.exe (266584)
 2 : |- EvernoteClipper.exe (336100)
 2 : |- EvernoteSubprocess.exe (92112)
 2 : EXCEL.EXE (174492)
 2 : |- splwow64.exe (203552)
 2 : AcroRd32.exe (19160)
 2 : |- AcroRd32.exe (18356)
 2 : |- RdrCEF.exe (18552)
 2 :    |- RdrCEF.exe (17556)
 2 :    |- RdrCEF.exe (18732)
 2 :    |- RdrCEF.exe (19572)
 2 :    |- RdrCEF.exe (19608)
 2 :    |- RdrCEF.exe (19844)
 2 :    |- RdrCEF.exe (215288)
 2 :    |- RdrCEF.exe (237228)
 2 :    |- RdrCEF.exe (291460)
 2 :    |- RdrCEF.exe (340876)
 2 : |- AdobeCollabSync.exe (73396)
 2 :    |- AdobeCollabSync.exe (16800)
 2 : LocalBridge.exe (199852)
 2 : firefox.exe (229412)
 2 : |- firefox.exe (128228)
 2 : |- firefox.exe (185180)
 2 : |- firefox.exe (227464)
 2 : |- firefox.exe (230268)
 2 : |- firefox.exe (299752)
 2 : OneDrive.exe (266156)
 2 : |- OneDrive.exe (41104)
 2 : chrome.exe (345536)
 2 : |- chrome.exe (116628)
 2 : |- chrome.exe (141072)
 2 : |- chrome.exe (150428)
 2 : |- chrome.exe (154768)
 2 : |- cmd.exe (155444)
 2 :    |- conhost.exe (298100)
 2 :    |- nplastpass.exe (341288)
 2 : |- chrome.exe (160308)
 2 : |- chrome.exe (165664)
 2 : |- chrome.exe (173680)
 2 : |- chrome.exe (175728)
 2 : |- chrome.exe (193632)
 2 : |- chrome.exe (19940)
 2 : |- chrome.exe (210148)
 2 : |- chrome.exe (218020)
 2 : |- chrome.exe (229084)
```

```
2 : |- chrome.exe (243620)
2 : |- chrome.exe (25404)
2 : |- chrome.exe (255052)
2 : |- chrome.exe (261816)
2 : |- chrome.exe (263968)
2 : |- chrome.exe (28264)
2 : |- [...]
```

125835 - Microsoft Remote Desktop Connection Installed

Synopsis

A graphical interface connection utility is installed on the remote Windows host

Description

Microsoft Remote Desktop Connection (also known as Remote Desktop Protocol or Terminal Services Client) is installed on the remote Windows host.

See Also

http://www.nessus.org/u?1c33f0e7

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2019/06/12, Modification date: 2019/11/22

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
Path    : C:\WINDOWS\\System32\\mstsc.exe
Version : 10.0.18362.752
```

65739 - Oracle Java JRE Universally Enabled

Synopsis

Oracle Java JRE has not been universally disabled on the remote host.

Description

Oracle Java JRE has not been universally disabled on the remote host via the Java control panel. Note that while Java can be individually disabled for each browser, universally disabling Java prevents it from running for all users and browsers.

See Also

https://www.java.com/en/download/help/disable_browser.xml

Solution

Disable Java universally unless it is needed.

Risk Factor

None

Plugin Information:

Publication date: 2013/03/29, Modification date: 2018/11/15

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

109730 - 7-Zip < 18.05 Memory Corruption Arbitrary Code Execution

Synopsis

A compression utility installed on the remote Windows host is affected by arbitrary code execution.

Description

The version of 7-Zip installed on the remote Windows host contains a flaw in the NArchive::NRar::CHandler::Extract method in Archive/Rar/RarHandler.cpp. The issue is triggered as certain input is not properly validated when performing 'solid' decompression of a RAR archive. With a specially crafted file, a context-dependent attacker can corrupt memory to cause a denial of service or potentially execute arbitrary code.

See Also

https://www.7-zip.org/history.txt

https://www.neowin.net/news/peazip-660

http://www.nessus.org/u?b2f13c3c

http://www.nessus.org/u?95f517fd

Solution

Upgrade to 7-Zip version 18.05 or later.

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

5.9

CVSS v3.0 Base Score

7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

6.8 (E:U/RL:O/RC:C)

CVSS Base Score

6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

5.0 (E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2018-10115
BID	104132
XREF	IAVA:2018-A-0147

Plugin Information:

Publication date: 2018/05/11, Modification date: 2019/11/04

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Path              : C:\Program Files\7-Zip
Installed version : 16.2.0.0
Fixed version     : 18.05
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

According to the MAC address of its network adapter, the remote host is a VMware virtual machine.

Solution

Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Risk Factor

None

Plugin Information:

Publication date: 2005/10/27, Modification date: 2019/12/11

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
The remote host is a VMware virtual machine.
```

56310 - Firewall Rule Enumeration

Synopsis

A firewall is configured on the remote host.

Description

Using the supplied credentials, Nessus was able to get a list of firewall rules from the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/09/28, Modification date: 2018/06/19

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
The following Firewall profiles are enabled on the remote Windows host:
  Public
Domain

By running "netsh", Nessus was able to get the
following list of firewall rules :


Rule Name:                            @{Microsoft.YourPhone_1.20061.110.0_x64__8wekyb3d8bbwe?ms-
resource://Microsoft.YourPhone/Resources/AppName}
----------------------------------------------------------------------
Description:                          @{Microsoft.YourPhone_1.20061.110.0_x64__8wekyb3d8bbwe?ms-
resource://Microsoft.YourPhone/Resources/AppName}
Enabled:                              Yes
Direction:                            In
Profiles:                             Domain,Private
Grouping:                             @{Microsoft.YourPhone_1.20061.110.0_x64__8wekyb3d8bbwe?ms-
resource://Microsoft.YourPhone/Resources/AppName}
LocalIP:                              Any
RemoteIP:                             Any
Protocol:                             Any
Edge traversal:                       No
InterfaceTypes:                       Any
Security:                             NotRequired
Rule source:                          Local Setting
Action:                               Allow

Rule Name:                            @{Microsoft.YourPhone_1.20061.110.0_x64__8wekyb3d8bbwe?ms-
resource://Microsoft.YourPhone/Resources/AppName}
----------------------------------------------------------------------
Description:                          @{Microsoft.YourPhone_1.20061.110.0_x64__8wekyb3d8bbwe?ms-
resource://Microsoft.YourPhone/Resources/AppName}
Enabled:                              Yes
Direction:                            Out
Profiles:                             Domain,Private,Public
Grouping:                             @{Microsoft.YourPhone_1.20061.110.0_x64__8wekyb3d8bbwe?ms-
resource://Microsoft.YourPhone/Resources/AppName}
LocalIP:                              Any
RemoteIP:                             Any
Protocol:                             Any
Edge traversal:                       No
InterfaceTypes:        [...]
```

24270 - Computer Manufacturer Information (WMI)

Synopsis

It is possible to obtain the name of the remote computer manufacturer.

Description

By making certain WMI queries, it is possible to obtain the model of the remote computer as well as the name of its manufacturer and its serial number.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/02/02, Modification date: 2020/06/23

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
Computer Manufacturer : VMware, Inc.
Computer Model : VMware Virtual Platform
Computer SerialNumber : VMware-ea 03 1a 42 4a b7 25 6b-dc 87 98 a0 20 4c 73 0c
Computer Type : Other

Computer Physical CPU's : 2
Computer Logical CPU's  : 4
  CPU0
    Architecture  : x64
    Physical Cores: 2
    Logical Cores : 2
  CPU1
    Architecture  : x64
    Physical Cores: 2
    Logical Cores : 2

Computer Memory : 16383 MB
  RAM slot #0
    Form Factor: DIMM
    Type       : DRAM
    Capacity   : 16384 MB
```

133049 - Security Update for Microsoft ASP.NET Core (January 2020)

Synopsis

The Microsoft ASP.NET Core installations on the remote host contain vulnerable packages.

Description

The Microsoft ASP.NET Core installation on the remote host is version 2.1.x < 2.1.15, 3.0.x < 3.0.2, or 3.1.x < 3.1.1. It is, therefore, affected by multiple vulnerabilities:
- A denial of service vulnerability exists when ASP.NET Core improperly handles web requests. An attacker who successfully exploited this vulnerability could cause a denial of service against an ASP.NET Core web application. The vulnerability can be exploited remotely, without authentication. A remote unauthenticated attacker could exploit this vulnerability by issuing specially crafted requests to the ASP.NET Core application. (CVE-2020-0602)
- A remote code execution vulnerability exists in ASP.NET Core software when the software fails to handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. (CVE-2020-0603)

See Also

http://www.nessus.org/u?530ba67f

http://www.nessus.org/u?374d2043

https://github.com/aspnet/Announcements/issues/402

https://github.com/aspnet/Announcements/issues/403

https://github.com/dotnet/aspnetcore/issues/18336

https://github.com/dotnet/aspnetcore/issues/18337

Solution

Update ASP.NET Core, remove vulnerable packages and refer to vendor advisory.

Risk Factor

High

Vulnerability Priority Rating (VPR)

5.9

CVSS v3.0 Base Score

8.8 (AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.7 (E:U/RL:O/RC:C)

CVSS Base Score

9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2020-0602
CVE	CVE-2020-0603
XREF	IAVA:2020-A-0027

Plugin Information:

Publication date: 2020/01/17, Modification date: 2020/01/20

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
  Path              : C:\Program Files\dotnet\shared\Microsoft.AspNetCore.App\2.1.4
  Installed version : 2.1.4

  Package           : Microsoft.AspNetCore.App
  Path              : C:\Program Files\dotnet\shared\Microsoft.AspNetCore.App\2.1.4
  Installed version : 2.1.4
  Fixed version     : 2.1.15

  Package           : Microsoft.AspNetCore.Http.Connections
  Path              : C:\Program Files\dotnet\shared\Microsoft.AspNetCore.App
\2.1.4\Microsoft.AspNetCore.Http.Connections.dll
  Installed version : 1.0.3.18207
  Fixed version     : 1.0.15
```

10902 - Microsoft Windows 'Administrators' Group User List

Synopsis

There is at least one user in the 'Administrators' group.

Description

Using the supplied credentials, it is possible to extract the member list of the 'Administrators' group. Members of this group have complete access to the remote system.

Solution

Verify that each member of the group should have this type of access.

Risk Factor

None

Plugin Information:

Publication date: 2002/03/15, Modification date: 2018/05/16

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
The following users are members of the 'Administrators' group :

  - VDA-IT-TS\Administrator (User)
  - VDA-IT-TS\ITaccount (User)
  - EDEN_MAIN\Domain Admins (Group)
  - EDEN_MAIN\ducati (User)
  - VDA-IT-TS\Tim (User)
  - EDEN_MAIN\t.styles (User)
  - VDA-IT-TS\SSRS_Reports (User)
  - VDA-IT-TS\SSIS_local (User)
  - EDEN_MAIN\a.meek (User)
  - EDEN_MAIN\IT Senior Admin (Group)
```

137271 - Security Updates for Microsoft Visual Studio Products (June 2020)

Synopsis

The Microsoft Visual Studio Products are affected by multiple vulnerabilities.

Description

The Microsoft Visual Studio Products are missing security updates. It is, therefore, affected by multiple vulnerabilities :
- An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector or the Visual Studio Standard Collector fail to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run processes in an elevated context. (CVE-2020-1202, CVE-2020-1203)
- An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector Service improperly handles file operations. An attacker who successfully exploited this vulnerability could gain elevated privileges. An attacker with unprivileged access to a vulnerable system could exploit this vulnerability. The security update addresses the vulnerability by ensuring the Diagnostics Hub Standard Collector Service properly handles file operations. (CVE-2020-1257, CVE-2020-1278, CVE-2020-1293)

See Also

http://www.nessus.org/u?cefba37b

http://www.nessus.org/u?702c8c2e

http://www.nessus.org/u?9f7a8135

http://www.nessus.org/u?8a60d006

http://www.nessus.org/u?edec5481

Solution

Microsoft has released the following security updates to address this issue:
- KB4562053 (for Visual Studio 2015)
- Update 15.9.24 for Visual Studio 2017
- Update 16.0.15 for Visual Studio 2019
- Update 16.4.10 for Visual Studio 2019
- Update 16.6.2 for Visual Studio 2019

Risk Factor

High

Vulnerability Priority Rating (VPR)

5.9

CVSS v3.0 Base Score

7.8 (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

6.8 (E:U/RL:O/RC:C)

CVSS Base Score

7.2 (AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

5.3 (E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2020-1278
CVE	CVE-2020-1202
CVE	CVE-2020-1257
CVE	CVE-2020-1203
CVE	CVE-2020-1293
XREF	MSKB:4562053
XREF	IAVA:2020-A-0257
XREF	MSFT:MS20-4562053

Plugin Information:

Publication date: 2020/06/09, Modification date: 2020/06/17

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
  Path              : C:\Program Files (x86)\Microsoft Visual Studio\2017\Community\Common7\IDE
\devenv.exe
  Installed version : 15.9.28307.1093
  Fixed version     : 15.9.28307.1177
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.
Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

https://nvd.nist.gov/products/cpe

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/04/21, Modification date: 2020/06/12

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
The remote operating system matched the following CPE :
```

```
  cpe:/o:microsoft:windows_10:::x64-enterprise

Following application CPE's matched on the remote system :

  cpe:/a:7-zip:7-zip:16.2.0.0
  cpe:/a:adobe:acrobat_reader:20.9.20067.384717
  cpe:/a:adobe:flash_player:32.0.0.387
  cpe:/a:evernote:evernote:6.25.1.9091
  cpe:/a:filezilla:filezilla:3.48.1.0
  cpe:/a:google:chrome:83.0.4103.116
  cpe:/a:microsoft:.net_core:2.1.202.0
  cpe:/a:microsoft:.net_core:2.1.402.0
  cpe:/a:microsoft:.net_core:2.1.513.0
  cpe:/a:microsoft:.net_framework:2.0.50727
  cpe:/a:microsoft:.net_framework:3.0 -> Microsoft .NET Framework 3.0
  cpe:/a:microsoft:.net_framework:3.5 -> Microsoft .net Framework 3.5
  cpe:/a:microsoft:.net_framework:4.8
  cpe:/a:microsoft:access:14.0.7248.5000
  cpe:/a:microsoft:access:16.0.12624.20466
  cpe:/a:microsoft:aspnet_core:2.0.13103.0
  cpe:/a:microsoft:aspnet_core:2.1.17
  cpe:/a:microsoft:aspnet_core:2.1.4
  cpe:/a:microsoft:edge:83.0.478.56
  cpe:/a:microsoft:excel:16.0.12624.20466
  cpe:/a:microsoft:ie:11.900.18362.0
  cpe:/a:microsoft:lync:16.0.12624.20466
  cpe:/a:microsoft:office:365
  cpe:/a:microsoft:office_compatibility_pack:
  cpe:/a:microsoft:office_compatibility_pack:14.0.4762.1000
  cpe:/a:microsoft:office_compatibility_pack:14.0.7248.5000
  cpe:/a:microsoft:office_compatibility_pack:16.0.12624.20466
  cpe:/a:microsoft:onenote:14.0.7172.5000
  cpe:/a:microsoft:powerpoint:16.0.12624.20466
  cpe:/a:microsoft:remote_desktop_connection:10.0.18362.752
  cpe:/a:microsoft:silverlight:5.1.50918.0
  cpe:/a:microsoft:sql_server:12.0.4522.0
  cpe:/a:microsoft:sql_server:13.0.4001.0
  cpe:/a:microsoft:sql_server_management_studio:2017.140.17289.0
  cpe:/a:microsoft:visio:14.0.7248.5000
  cpe:/a:microsoft:visio_viewer:14.0.7163.5000
  cpe:/a:microsoft:visio_viewer:16.0.12624.20422
  cpe:/a:microsoft:visual_studio:10.0.40219.1
  cpe:/a:microsoft:visual_studio:11.0.61219.0
  cpe:/a:microsoft:visual_studio:12.0.40629.0
  cpe:/a:microsoft:visual_studio:15.9.28307.1093
  [...]
```

70331 - Microsoft Windows Process Module Information

Synopsis

Use WMI to obtain running process module information.

Description

Report details on the running processes modules on the machine.
This plugin is informative only and could be used for forensic investigation, malware detection, and to that confirm your system processes conform to your system policies.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/10/08, Modification date: 2020/06/23

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
Process_Modules_VDA-IT-TS.edenbrown.uk.csv : lists the loaded modules for each process.
```

24269 - WMI Available

Synopsis

WMI queries can be made against the remote host.

Description

The supplied credentials can be used to make WMI (Windows Management Instrumentation) requests against the remote host over DCOM.
These requests can be used to gather information about the remote host, such as its current state, network interface configuration, etc.

See Also

https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/02/03, Modification date: 2020/06/23

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
The remote host returned the following caption from Win32_OperatingSystem:

 Microsoft Windows 10 Enterprise
```

92431 - User Shell Folders Settings

Synopsis

Nessus was able to find the folder paths for user folders on the remote host.

Description

Nessus was able to gather a list of settings from the target system that store common user folder locations. A few of the more common locations are listed below :
- Administrative Tools
- AppData
- Cache
- CD Burning
- Cookies
- Desktop
- Favorites
- Fonts
- History
- Local AppData
- My Music
- My Pictures
- My Video
- NetHood
- Personal
- PrintHood
- Programs
- Recent
- SendTo
- Start Menu
- Startup
- Templates

See Also

https://technet.microsoft.com/en-us/library/cc962613.aspx

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2018/05/16

Ports

vda-it-ts (TCP/0) Vulnerability State: Resurfaced

```
 EDENBROWN.UK\t.styles
  - {7d1d3a04-debb-4115-95cf-2f29da2920da} : C:\Users\t.styles\Searches
  - {1b3ea5dc-b587-4786-b4ef-bd1dc332aeae} : C:\Users\t.styles\AppData\Roaming\Microsoft\Windows
\Libraries
  - {374de290-123f-4565-9164-39c4925e467b} : C:\Users\t.styles\Downloads
  - recent : C:\Users\t.styles\AppData\Roaming\Microsoft\Windows\Recent
  - my video : C:\Users\t.styles\Videos
  - my music : C:\Users\t.styles\Music
  - {56784854-c6cb-462b-8169-88e350acb882} : C:\Users\t.styles\Contacts
  - {bfb9d5e0-c6a9-404c-b2b2-ae6db6af4968} : C:\Users\t.styles\Links
  - {a520a1a4-1780-4ff6-bd18-167343c5af16} : C:\Users\t.styles\AppData\LocalLow
  - sendto : C:\Users\t.styles\AppData\Roaming\Microsoft\Windows\SendTo
  - start menu : C:\Users\t.styles\AppData\Roaming\Microsoft\Windows\Start Menu
  - cookies : C:\Users\t.styles\AppData\Local\Microsoft\Windows\INetCookies
  - personal : C:\Users\t.styles\Documents
  - administrative tools : C:\Users\t.styles\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
\Administrative Tools
  - startup : C:\Users\t.styles\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
  - nethood : C:\Users\t.styles\AppData\Roaming\Microsoft\Windows\Network Shortcuts
  - history : C:\Users\t.styles\AppData\Local\Microsoft\Windows\History
  - {4c5c32ff-bb9d-43b0-b5b4-2d72e54eaaa4} : C:\Users\t.styles\Saved Games
  - {00bcfc5a-ed94-4e48-96a1-3f6217f21990} : C:\Users\t.styles\AppData\Local\Microsoft\Windows
\RoamingTiles
  - !do not use this registry key : Use the SHGetFolderPath or SHGetKnownFolderPath function
 instead
  - local appdata : C:\Users\t.styles\AppData\Local
  - my pictures : C:\Users\t.styles\Pictures
  - templates : C:\Users\t.styles\AppData\Roaming\Microsoft\Windows\Templates
  - printhood : C:\Users\t.styles\AppData\Roaming\Microsoft\Windows\Printer Shortcuts
  - cache : C:\Users\t.styles\AppData\Local\Microsoft\Windows\INetCache
  - desktop : C:\Users\t.styles\Desktop
  - programs : C:\Users\t.styles\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
  - fonts : [...]
```

92435 - UserAssist Execution History

Synopsis

Nessus was able to enumerate program execution history on the remote host.

Description

Nessus was able to gather evidence from the UserAssist registry key that has a list of programs that have been executed.

See Also

https://www.nirsoft.net/utils/userassist_view.html

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2019/11/12

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
 c:\users\t.styles\appdata\local\temp\vs\setup
\3b65be0a-98e9-4c4d-82b0-4d609c7ec059\vs_setup_bootstrapper.exe
c:\users\t.styles\appdata\local\temp\netwrixtempfiles\autorun.exe
c:\users\t.styles\downloads\readerdc_uk_a_install.exe
c:\users\t.styles\appdata\local\microsoft\onedrive\onedrive.exe
c:\users\t.styles\desktop\postman.lnk
{6d809377-6af0-444b-8957-a3773f02200e}\sqlyog\sqlyog.exe
microsoft.aad.brokerplugin_cw5n1h2txyewy!app
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\dsa.msc
visualstudio.12.0
microsoft.internetexplorer.default
```

```
chrome.scopeddir25498830801.default
{9e3995ab-1f9c-4f13-b827-48b24b6c7174}\taskbar\mat.ui.lnk
chrome.userdata.guestprofile
{6d809377-6af0-444b-8957-a3773f02200e}\common files\microsoft shared\clicktorun
\officeclicktorun.exe
c:\users\t.styles\downloads\filezilla_3.48.1_win64-setup.exe
{a77f5d77-2e2b-44c3-a6a2-aba601054a51}\onedrive.lnk
microsoft.office.explorer.exe.15
microsoft.zunevideo_8wekyb3d8bbwe!microsoft.zunevideo
{0139d44e-6afe-49f2-8690-3dafcae6ffb8}\microsoft sql server tools 17\microsoft sql server
 management studio 17.lnk
msedge
c:\users\t.styles\downloads\filezilla_3.48.0_win64-setup.exe
{0139d44e-6afe-49f2-8690-3dafcae6ffb8}\visual studio 2017.lnk
{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}\sophos\sophos diagnostic utility\sdugui.exe
microsoft.windows.startmenuexperiencehost_cw5n1h2txyewy!app
_crx_cplklnmnlbncfgfijoopmnlemp.userdata.default
{9e3995ab-1f9c-4f13-b827-48b24b6c7174}\taskbar\slack.lnk
com.squirrel.postman.postman
c:\users\t.styles\appdata\local\slack\app-4.0.2\slack.exe
c:\users\t.styles\downloads\filezilla_3.47.1_win64-setup.exe
{9e3995ab-1f9c-4f13-b827-48b24b6c7174}\taskbar\evernote.lnk
visualstudio.ed3fddd6
\\data01\itdept$\_new itdept\dba-team\software\pragmaticworks\version
 2019.1.2\taskfactory_version_2019_1_2\taskfactory - version 2019.1.2.exe
c:\users\t.styles\appdata\local\temp\temp2_mat 3.4.8 [...]
```

131023 - Windows Defender Installed

Synopsis

Windows Defender is installed on the remote Windows host.

Description

Windows Defender, an antivirus component of Microsoft Windows is installed on the remote Windows host.

See Also

https://www.microsoft.com/en-us/windows/comprehensive-security

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2019/11/15, Modification date: 2020/06/23

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
  Path                        : C:\ProgramData\Microsoft\Windows Defender\platform\4.18.1903.3-0\
  Version                     : 4.18.1903.3
  Disabled                    : 1
  Engine Version              : 1.1.16300.1
  Malware Signature Timestamp : Sep.  9, 2019 at 04:21:27 GMT
  Malware Signature Version   : 1.301.845.0
  Signatures Last Updated     : Sep.  9, 2019 at 07:27:43 GMT
```

91231 - 7-Zip Installed

Synopsis

A compression utility is installed on the remote Windows host.

Description

7-Zip, a compressed archive manager, is installed on the remote Windows host.

See Also

https://www.7-zip.org/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/05/19, Modification date: 2020/06/23

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
  Path    : C:\Program Files\7-Zip
  Version : 16.2.0.0
```

104667 - Microsoft ASP .NET Core for Windows

Synopsis

ASP .NET Core runtime packages are installed on the remote Windows host.

Description

ASP .NET Core runtime, web application server side components, are installed on the remote Windows host.

See Also

https://github.com/aspnet/AspNetCore

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2017/11/17, Modification date: 2020/06/23

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Nessus detected 5 installs of ASP .NET Core Windows:

  Path    : C:\Program Files\dotnet\shared\Microsoft.AspNetCore.App\2.1.4
  Version : 2.1.4

  Path    : C:\Program Files\dotnet\store\x64\netcoreapp2.0
  Version : 2.0.13103.0

  Path    : C:\Program Files\dotnet\shared\Microsoft.AspNetCore.App\2.1.17
  Version : 2.1.17

  Path    : C:\Program Files\dotnet\shared\Microsoft.AspNetCore.All\2.1.17
  Version : 2.1.17

  Path    : C:\Program Files\dotnet\shared\Microsoft.AspNetCore.All\2.1.4
  Version : 2.1.4
```

109029 - Security Updates for Microsoft Visual Studio Products (April 2018)

Synopsis

The Microsoft Visual Studio Products are missing a security update.

Description

The Microsoft Visual Studio Products are missing a security update. It is, therefore, affected by the following vulnerability :
- An information disclosure vulnerability exists when Visual Studio improperly discloses limited contents of uninitialized memory while compiling program database (PDB) files. An attacker who took advantage of this information disclosure could view uninitialized memory from the Visual Studio instance used to compile the PDB file. To take advantage of the vulnerability, an attacker would require access to an affected PDB file created using a vulnerable version of Visual Studio. An attacker would have no way to force a developer to produce this information disclosure. The security update addresses the vulnerability by correcting how PDB files are generated when a project is compiled. (CVE-2018-1037)

See Also

http://www.nessus.org/u?1a8e7d73

http://www.nessus.org/u?5b4e94bf

http://www.nessus.org/u?b61645d0

http://www.nessus.org/u?de1ae25a

Solution

Microsoft has released the following security updates to address this issue:
-KB4089501
-KB4091346
-KB4087371
-KB4089283

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

1.4

CVSS v3.0 Base Score

4.3 (AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N)

CVSS v3.0 Temporal Score

3.8 (E:U/RL:O/RC:C)

CVSS Base Score

4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

3.2 (E:U/RL:OF/RC:C)

References

CVE	CVE-2018-1037
BID	103715
XREF	MSKB:4089501
XREF	MSFT:MS18-4089283
XREF	MSKB:4087371
XREF	MSFT:MS18-4091346
XREF	MSFT:MS18-4089501
XREF	MSFT:MS18-4087371
XREF	MSKB:4091346
XREF	MSKB:4089283

Plugin Information:

Publication date: 2018/04/13, Modification date: 2019/11/08

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Path              : C:\Program Files (x86)\Microsoft Visual Studio 12.0\VC\bin\mspdbsrv.exe
Installed version : 12.0.40629.0
Fixed version     : 12.0.40669.0
```

132101 - Windows Speculative Execution Configuration Check

Synopsis

The remote host has not properly mitigated a series of speculative execution vulnerabilities.

Description

The remote host has not properly mitigated a series of known speculative execution vulnerabilities. It, therefore, may be affected by :
- Branch Target Injection (BTI) (CVE-2017-5715)
- Bounds Check Bypass (BCB) (CVE-2017-5753)
- Rogue Data Cache Load (RDCL) (CVE-2017-5754)
- Rogue System Register Read (RSRE) (CVE-2018-3640)
- Speculative Store Bypass (SSB) (CVE-2018-3639)
- L1 Terminal Fault (L1TF) (CVE-2018-3615, CVE-2018-3620, CVE-2018-3646)
- Microarchitectural Data Sampling Uncacheable Memory (MDSUM) (CVE-2019-11091)
- Microarchitectural Store Buffer Data Sampling (MSBDS) (CVE-2018-12126)
- Microarchitectural Load Port Data Sampling (MLPDS) (CVE-2018-12127)
- Microarchitectural Fill Buffer Data Sampling (MFBDS) (CVE-2018-12130)
- TSX Asynchronous Abort (TAA) (CVE-2019-11135)

See Also

http://www.nessus.org/u?8902cebb

http://www.nessus.org/u?6a005ed4

Solution

Apply vendor recommended settings.

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

8.3

CVSS v3.0 Base Score

6.4 (AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:L/A:N)

CVSS v3.0 Temporal Score

6.1 (E:H/RL:O/RC:C)

CVSS Base Score

5.4 (AV:L/AC:M/Au:N/C:C/I:P/A:N)

CVSS Temporal Score

4.7 (E:H/RL:OF/RC:C)

References

CVE	CVE-2018-3620
CVE	CVE-2017-5753
CVE	CVE-2018-12127
CVE	CVE-2017-5754
CVE	CVE-2019-11135
CVE	CVE-2018-3639
CVE	CVE-2018-3615
CVE	CVE-2018-12126
CVE	CVE-2018-3646
CVE	CVE-2018-12130

CVE	CVE-2017-5715
BID	102371
BID	104232
BID	105080
BID	102378
BID	108330

Exploitable with

CANVAS

Plugin Information:

Publication date: 2019/12/18, Modification date: 2020/06/12

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Current Settings:
  - SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\
    FeatureSettingsOverrideMask: Not Set
  - SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\
    FeatureSettingsOverride: Not Set

-----------------------------------

Recommended Settings 1:
  - SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\
    FeatureSettingsOverrideMask: 0x00000003 (3)
  - SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\
    FeatureSettingsOverride: 0x00000008 (8)
  CVEs Covered:
    CVE-2017-5715, CVE-2017-5754, CVE-2018-3639
  Note: Remaining protections enabled by default on clients. Required for CVE-2018-3639.

-----------------------------------

Recommended Settings 2:
  - SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\
    FeatureSettingsOverrideMask: 0x00000003 (3)
  - SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\
    FeatureSettingsOverride: 0x00000048 (72)
  CVEs Covered:
    CVE-2017-5715, CVE-2017-5753, CVE-2017-5754, CVE-2018-3615, CVE-2018-3620,
    CVE-2018-3639, CVE-2018-3646, CVE-2018-11091, CVE-2018-12126, CVE-2018-12127,
    CVE-2018-12130, CVE-2019-11135
  Note: Hyper-Threading enabled.
  Note: Most protections enabled by default on clients. Required for CVE-2018-3639.

-----------------------------------

Recommended Settings 3:
  - SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\
    FeatureSettingsOverrideMask: 0x00000003 (3)
  - SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\
    FeatureSettingsOverride: 0x00002048 (8264)
  CVEs Covered:
    CVE-2017-5715, CVE-2017-5753, CVE-2017-5754, CVE-2018-3615, CVE-2018-3620,
    CVE-2018-3639, CVE-2018-3646, CVE-2018-11091, CVE-2018-12126, CVE-2018-12127,
    CVE-2018-12130, CVE-2019-11135
  Note: Hyper-Threading disabled.
  Note: Most protections enabled by default on clients. Required for CVE-2018-3639.
```

20836 - Adobe Reader Detection

Synopsis

There is a PDF file viewer installed on the remote Windows host.

Description

Adobe Reader, a PDF file viewer, is installed on the remote host.

See Also

http://www.adobe.com/products/reader/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2006/02/02, Modification date: 2019/11/22

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
  Path    : C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader
  Version : 20.9.20067.384717
```

63080 - Microsoft Windows Mounted Devices

Synopsis

It is possible to get a list of mounted devices that may have been connected to the remote system in the past.

Description

By connecting to the remote host with the supplied credentials, this plugin enumerates mounted devices that have been connected to the remote host in the past.

See Also

http://www.nessus.org/u?99fcc329

Solution

Make sure that the mounted drives agree with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Publication date: 2012/11/28, Modification date: 2019/11/22

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
  Name     : \??\volume{edef350b-bdb2-11e3-948b-534e57000000}
  Data     : Y$~
  Raw data : d75924a5007e000000000000

  Name     : \??\volume{268940f1-aa8b-11e3-ac5f-534e57000000}
  Data     : \??\SCSI#CdRom&Ven_MagicISO&Prod_Virtual_DVD-
ROM&Rev_1.0A#1&2afd7d61&0&0000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
  Raw data :
 5c003f003f005c005300430053004900230043006400520006f006d002600560065006e005f004d006100670069006300490053004f002

  Name     : \??\volume{3b535288-0d0f-11e6-9c2a-001c423120d1}
  Data     : _??_USBSTOR#Disk&Ven_USB&Prod_DISK&Rev_5.00#130905090502386816710 1&0#{53f56307-
b6bf-11d0-94f2-00a0c91efb8b}
  Raw data :
 5f003f003f005f005500530042005300540 04f005200230044006900730 06b002600560065006e005f005500530042002600500072006

  Name     : \??\volume{c7f38483-74b3-11e3-adb5-806e6f6e6963}
  Data     : GV
  Raw data : d047cd560000100000000000

  Name     : \??\volume{3103c54a-7471-11e3-b99c-806e6f6e6963}
  Data     : \??\IDE#CdRom_Virtual_DVD-
ROM_____R103____#5&23d521a4&0&1.0.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
  Raw data : [...]
```

111072 - Microsoft ASP.NET Core Privilege Escalation (March 2018)

Synopsis

The Microsoft ASP.NET Core installations on the remote host contain vulnerable packages.

Description

The remote Windows host has an installation of ASP.NET Core containing the packages HttpOverrides and/or Server.Kestrel.Core with versions 2.0.0 or 2.0.1 and therefore is affected by a privilege escalation vulnerability.

See Also

https://github.com/aspnet/Announcements/issues/295

http://www.nessus.org/u?eda99e15

Solution

Update HttpOverrides and/or Server.Kestrel.Core to version 2.0.2, remove the vulnerable versions and refer to the vendor advisory.

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

6.7

CVSS v3.0 Base Score

8.8 (AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.7 (E:U/RL:O/RC:C)

CVSS Base Score

6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

5.0 (E:U/RL:OF/RC:C)

References

CVE	CVE-2018-0787
BID	103282

Plugin Information:

Publication date: 2018/07/13, Modification date: 2019/11/04

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
  Path              : C:\Program Files\dotnet\store\x64\netcoreapp2.0
  Installed version : 2.0.13103.0

  Package           : Microsoft.AspNetCore.Server.Kestrel.Core
  Path              : C:\Program Files\dotnet\store
\x64\netcoreapp2.0\microsoft.aspnetcore.server.kestrel.core\2.0.0\lib
\netstandard2.0\Microsoft.AspNetCore.Server.Kestrel.Core.dll
  Installed version : 2.0.0.17205
  Fixed version     : 2.0.2

  Package           : Microsoft.AspNetCore.Server.Kestrel.Core
  Path              : C:\Program Files\dotnet\store
\x64\netcoreapp2.0\microsoft.aspnetcore.server.kestrel.core\2.0.1\lib
\netstandard2.0\Microsoft.AspNetCore.Server.Kestrel.Core.dll
  Installed version : 2.0.1.17303
  Fixed version     : 2.0.2

  Package           : Microsoft.AspNetCore.HttpOverrides
  Path              : C:\Program Files\dotnet\store
\x64\netcoreapp2.0\microsoft.aspnetcore.httpoverrides\2.0.0\lib
\netstandard2.0\Microsoft.AspNetCore.HttpOverrides.dll
  Installed version : 2.0.0.17205
  Fixed version     : 2.0.2
```

```
  Package           : Microsoft.AspNetCore.HttpOverrides
  Path              : C:\Program Files\dotnet\store
\x64\netcoreapp2.0\microsoft.aspnetcore.httpoverrides\2.0.1\lib
\netstandard2.0\Microsoft.AspNetCore.HttpOverrides.dll
  Installed version : 2.0.1.17303
  Fixed version     : 2.0.2
```

77605 - Microsoft OneNote Detection

Synopsis

The remote Windows host contains Microsoft OneNote.

Description

Microsoft OneNote is installed on the remote host.

See Also

https://www.onenote.com/signin?wdorigin=ondc

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2014/09/10, Modification date: 2020/06/12

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
  Path    : C:\Program Files\Microsoft Office\Office14\OneNote.exe
  Version : 14.0.7172.5000
```

103871 - Microsoft Windows Network Adapters

Synopsis

Identifies the network adapters installed on the remote host.

Description

Using the supplied credentials, this plugin enumerates and reports the installed network adapters on the remote Windows host.

Solution

Make sure that all of the installed network adapters agrees with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Publication date: 2017/10/17, Modification date: 2020/05/15

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Network Adapter Driver Description : vmxnet3 Ethernet Adapter
Network Adapter Driver Version     : 1.8.10.0
```

124651 - Oracle Java File Detection for Windows

Synopsis

Detected Java files on the host

Description

The host contains one or more java executables.

See Also

https://www.oracle.com/technetwork/java/index.html

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2019/05/06, Modification date: 2020/06/23

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
Java files found: 13
 - C:\Documents and Settings\All Users\Oracle\Java\javapath\java.exe
 - C:\Documents and Settings\All Users\Oracle\Java\javapath_target_529031\java.exe
 - C:\Program Files (x86)\Java\jdk1.8.0_181\bin\java.exe
 - C:\Program Files (x86)\Java\jdk1.8.0_181\jre\bin\java.exe
 - C:\Program Files\Android\jdk\microsoft_dist_openjdk_1.8.0.25\bin\java.exe
 - C:\Program Files\Android\jdk\microsoft_dist_openjdk_1.8.0.25\jre\bin\java.exe
 - C:\Program Files\DBeaver\jre\bin\java.exe
 - C:\Program Files\Java\jdk1.8.0_181\bin\java.exe
 - C:\Program Files\Java\jdk1.8.0_181\jre\bin\java.exe
 - C:\ProgramData\Oracle\Java\javapath\java.exe
 - C:\ProgramData\Oracle\Java\javapath_target_529031\java.exe
 - C:\Users\All Users\Oracle\Java\javapath\java.exe
 - C:\Users\All Users\Oracle\Java\javapath_target_529031\java.exe
```

62758 - Microsoft XML Parser (MSXML) and XML Core Services Unsupported

Synopsis

The remote Windows host contains unsupported XML parsers.

Description

The remote host contains one or more unsupported versions of the Microsoft XML Parser (MSXML) or XML Core Services.
Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.
Note that support for MSXML 3.0 and 6.0 is based on the support policy of the operating system on which it is installed. Support for MSXML 5.0 is based on the Microsoft Office lifecycle policy.

See Also

http://www.nessus.org/u?92132729

http://www.nessus.org/u?cfb1b524

Solution

Upgrade the software packages responsible for the unsupported DLL versions or upgrade to a supported version of Windows (Vista / 2008 or later). Alternatively, uninstall the outdated MSXML or XML Core Services.

Risk Factor

Critical

CVSS v3.0 Base Score

10.0 (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

CVSS Base Score

10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Information:

Publication date: 2012/10/30, Modification date: 2019/04/26

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Path               : C:\WINDOWS\SysWOW64\msxml4.dll
File version       : 4.20.9876.0
XML Core version   : 4.0 Post SP3 (KB2758694)
EOL date           : 2014/04/12
EOL announcement   : https://support.microsoft.com/en-us/lifecycle/search/7921
```

```
  Supported versions : 5.20.1076 (Office 2007) / 6.0 or later on a supported version of Windows
(Vista / 2008 or later).
```

135718 - Security Updates for Microsoft Defender (April 2020)

Synopsis

An antimalware application installed on the remote host is affected by an elevation of privilege vulnerability.

Description

The version of Microsoft Malware Protection Signature Update Stub (MpSigStub.exe) installed on the remote Windows host is prior to 1.1.16638.0. It is, therefore, affected by a elevation of privilege vulnerability which could allow an attacker who successfully exploited this vulnerability to elevate privileges on the system.

See Also

http://www.nessus.org/u?d6966f51

Solution

Enable automatic updates to update the scan engine for the relevant antimalware applications. Refer to Knowledge Base Article 2510781 for information on how to verify that MMPE has been updated.

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

7.7

CVSS v3.0 Base Score

7.1 (AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H)

CVSS v3.0 Temporal Score

6.2 (E:U/RL:O/RC:C)

CVSS Base Score

6.6 (AV:L/AC:L/Au:N/C:N/I:C/A:C)

CVSS Temporal Score

4.9 (E:U/RL:OF/RC:C)

References

CVE	CVE-2020-1002

Plugin Information:

Publication date: 2020/04/17, Modification date: 2020/04/23

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
Product           : Microsoft Malware Protection Signature Update Stub
Path              : C:\WINDOWS\System32\MpSigStub.exe
Installed version : 1.1.16200.1
Fixed version     : 1.1.16638.0
```

92365 - Microsoft Windows Hosts File

Synopsis

Nessus was able to collect the hosts file from the remote host.

Description

Nessus was able to collect the hosts file from the remote Windows host and report it as attachment.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2020/01/27

Ports
vda-it-ts (TCP/0) Vulnerability State: Active

```
Windows hosts file attached.

MD5: ca9a7f936bd325fff38bc74cde855932
SHA-1: 23794a275be09e938146274e7c0661f8b019e740
SHA-256: 866d03fef97bc9693c39486fd1bdc9ae0d68eb05d50d9ad70bd7f3968714dfbe
```

92369 - Microsoft Windows Time Zone Information

Synopsis

Nessus was able to collect and report time zone information from the remote host.

Description

Nesssus was able to collect time zone information from the remote Windows host and generate a report as a CSV attachment.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2020/06/12

Ports
vda-it-ts (TCP/0) Vulnerability State: Active

```
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\TimeZoneKeyName : GMT Standard Time
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\StandardName : @tzres.dll,-262
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\DaylightName : @tzres.dll,-261
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\DynamicDaylightTimeDisabled : 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\StandardBias : 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\DaylightBias : 0xFFFFFFC4
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\Bias : 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\ActiveTimeBias : 0xFFFFFFC4
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\DaylightStart :
 00000300050001000000000000000000
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\StandardStart :
 00000a0005000200000000000000000
```

92428 - Recent File History

Synopsis

Nessus was able to enumerate recently opened files on the remote host.

Description

Nessus was able to gather evidence of files opened by file type from the remote host.

See Also

https://www.4n6k.com/2014/02/forensics-quickie-pinpointing-recent.html

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2018/11/15

Ports
vda-it-ts (TCP/0) Vulnerability State: Resurfaced

```
C:\\Users\Tim\AppData\Roaming\Microsoft\Windows\Recent\Summary of In house IT Development work
 from June 2013.lnk

Recent files found in registry and appdata attached.
```

92419 - Flash Cookie History

Synopsis

Nessus was able to gather Flash cookie URL history on the remote host.

Description

Nessus was able to generate a list of URLs that set Flash cookies on the remote host.

See Also

http://www.nessus.org/u?59436209

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2018/05/23

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
 C:\\Users\t.styles\AppData\Roaming\Macromedia\Flash Player\#SharedObjects\Y9Y85DDK\#AppContainer\
C:\\Users\t.styles\AppData\Roaming\Macromedia\Flash Player\#SharedObjects\Y9Y85DDK\aa.online-
metrix.net\
C:\\Users\t.styles\AppData\Roaming\Macromedia\Flash Player\#SharedObjects\Y9Y85DDK
\admin.brightcove.com\
C:\\Users\t.styles\AppData\Roaming\Macromedia\Flash Player\#SharedObjects\Y9Y85DDK
\aka.spotxcdn.com\
C:\\Users\t.styles\AppData\Roaming\Macromedia\Flash Player\#SharedObjects\Y9Y85DDK
\api.inspiredlabs.com\
C:\\Users\t.styles\AppData\Roaming\Macromedia\Flash Player\#SharedObjects\Y9Y85DDK
\cdn.stickyadstv.com\
C:\\Users\t.styles\AppData\Roaming\Macromedia\Flash Player\#SharedObjects\Y9Y85DDK\cdns.canddi.com
\
C:\\Users\t.styles\AppData\Roaming\Macromedia\Flash Player\#SharedObjects\Y9Y85DDK\emp.bbci.co.uk\
C:\\Users\t.styles\AppData\Roaming\Macromedia\Flash Player\#SharedObjects\Y9Y85DDK\images-eu.ssl-
images-amazon.com\
C:\\Users\t.styles\AppData\Roaming\Macromedia\Flash Player\#SharedObjects\Y9Y85DDK\images-na.ssl-
images-amazon.com\
C:\\Users\t.styles\AppData\Roaming\Macromedia\Flash Player\#SharedObjects\Y9Y85DDK
\mpsnare.iesnare.com\
C:\\Users\t.styles\AppData\Roaming\Macromedia\Flash Player\#SharedObjects\Y9Y85DDK
\qsf.is.quoracdn.net\
C:\\Users\t.styles\AppData\Roaming\Macromedia\Flash Player\#SharedObjects\Y9Y85DDK\s.ytimg.com\
C:\\Users\t.styles\AppData\Roaming\Macromedia\Flash Player\#SharedObjects\Y9Y85DDK
\scontent.lrcdn.net\
C:\\Users\t.styles\AppData\Roaming\Macromedia\Flash Player\#SharedObjects\Y9Y85DDK
\securesuite.co.uk\
C:\\Users\t.styles\AppData\Roaming\Macromedia\Flash Player\#SharedObjects\Y9Y85DDK\skype.com\
C:\\Users\t.styles\AppData\Roaming\Macromedia\Flash Player\#SharedObjects\Y9Y85DDK
\video.sekindo.com\
C:\\Users\t.styles\AppData\Roaming\Macromedia\Flash Player\#SharedObjects\Y9Y85DDK\vox-
static.liverail.com\
C:\\Users\t.styles\AppData\Roaming\Macromedia\Flash Player\#SharedObjects\Y9Y85DDK\www.cdn-net.com
\
C:\\Users\t.styles\AppData\Roaming\Macromedia\Flash [...]
```

118095 - Microsoft SQL Server Management Studio (SSMS) Installed

Synopsis

A SQL Server Management solution is installed on the remote Windows host.

Description

Microsoft SQL Server Management Studio (SSMS) is installed on the remote Windows host.

See Also

http://www.nessus.org/u?00f3184c

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2018/10/12, Modification date: 2020/06/23

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
Path    : C:\Program Files (x86)\Microsoft SQL Server\140\Tools\Binn\ManagementStudio\
Version : 2017.140.17289.0
```

111070 - Security Updates for Microsoft .NET core and ASP.NET (Bypass) (July 2018)

Synopsis

The Microsoft ASP.NET Core installations on the remote host contain vulnerable packages.

Description

The Microsoft .NET and ASP.NET installations on the remote host are missing a security update. It is, therefore, affected by the following vulnerability :
- A Security Feature Bypass vulnerability exists in ASP.NET when the number of incorrect login attempts is not validated. An attacker who successfully exploited this vulnerability could try an infinite number of authentication attempts. The update addresses the vulnerability by validating the number of incorrect login attempts. (CVE-2018-8171)

See Also

http://www.nessus.org/u?59900f80

https://github.com/aspnet/Announcements/issues/310

Solution

Update ASP.NET Core, remove vulnerable packages and refer to vendor advisory.

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

3.6

CVSS v3.0 Base Score

7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N)

CVSS v3.0 Temporal Score

6.5 (E:U/RL:O/RC:C)

CVSS Base Score

5.0 (AV:N/AC:L/Au:N/C:N/I:P/A:N)

CVSS Temporal Score

3.7 (E:U/RL:OF/RC:C)

References

CVE	CVE-2018-8171
BID	104659
XREF	MSKB:4339279
XREF	MSFT:MS18-4339279

Plugin Information:

Publication date: 2018/07/13, Modification date: 2019/11/04

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Path              : C:\Program Files\dotnet\store\x64\netcoreapp2.0
Installed version : 2.0.13103.0
```

```
  Package           : Microsoft.AspNetCore.Identity
  Path              : C:\Program Files\dotnet\store
\x64\netcoreapp2.0\microsoft.aspnetcore.identity\2.0.0\lib
\netstandard2.0\Microsoft.AspNetCore.Identity.dll
  Installed version : 2.0.0.17205
  Fixed version     : 2.0.4

  Package           : Microsoft.AspNetCore.Identity
  Path              : C:\Program Files\dotnet\store
\x64\netcoreapp2.0\microsoft.aspnetcore.identity\2.0.1\lib
\netstandard2.0\Microsoft.AspNetCore.Identity.dll
  Installed version : 2.0.1.17303
  Fixed version     : 2.0.4

  Package           : Microsoft.AspNetCore.Identity
  Path              : C:\Program Files\dotnet\store
\x64\netcoreapp2.0\microsoft.aspnetcore.identity\2.0.2\lib
\netstandard2.0\Microsoft.AspNetCore.Identity.dll
  Installed version : 2.0.2.18051
  Fixed version     : 2.0.4

  Package           : Microsoft.AspNetCore.Identity
  Path              : C:\Program Files\dotnet\store
\x64\netcoreapp2.0\microsoft.aspnetcore.identity\2.0.3\lib
\netstandard2.0\Microsoft.AspNetCore.Identity.dll
  Installed version : 2.0.3.18114
  Fixed version     : 2.0.4
```

23974 - Microsoft Windows SMB Share Hosting Office Files

Synopsis

The remote share contains Office-related files.

Description

This plugin connects to the remotely accessible SMB shares and attempts to find office related files (such as .doc, .ppt, .xls, .pdf etc).

Solution

Make sure that the files containing confidential information have proper access controls set on them.

Risk Factor

None

Plugin Information:

Publication date: 2007/01/04, Modification date: 2011/03/21

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Here is a list of office files which have been found on the remote SMB
shares :

  + C$ :

    - \Program Files\Microsoft Office\root\Office16\1033\PROTTPLV.DOC
    - \$Recycle.Bin\S-1-5-21-330363374-4240072399-3876068862-1001\$RF9T70C.styles\AppData\Roaming
\Microsoft\Templates\Doc1.doc
    - \Microsoft\AndroidNDK64\android-ndk-r15c\prebuilt\windows-x86_64\lib\python2.7\pdb.doc
    - \Program Files\Microsoft Office\Office14\1033\PROTTPLN.DOC
    - \Program Files\Microsoft Office\Office14\1033\PROTTPLV.DOC
    - \Program Files\Microsoft Office\root\Office16\1033\PROTTPLN.DOC
    - \Program Files (x86)\Microsoft Visual Studio\Shared\Packages
\Microsoft.SqlServer.Compact.4.0.8876.1\SQLCE_EULA_ENU.rtf
    - \Program Files (x86)\Microsoft Visual Studio\Shared\Packages
\Microsoft.Net.Http.2.2.29\License-Stable.rtf
    - \Program Files (x86)\Microsoft Visual Studio\Shared\Packages
\Microsoft.Bcl.Async.1.0.168\License-Stable.rtf
    - \Program Files (x86)\Microsoft Visual Studio\Shared\Packages\Microsoft.Bcl.1.1.9\License-
Stable.rtf
    - \Program Files (x86)\Microsoft Visual Studio\Shared\Packages\Microsoft.Bcl.1.1.10\License-
Stable.rtf
    - \Program Files (x86)\Microsoft Visual Studio\Shared\eula.rtf
```

```
   - \Program Files (x86)\Microsoft Visual Studio\2017\Community\Licenses\Windows 8.1 SDK Third
Party Notices.rtf
   - \Program Files (x86)\Microsoft Visual Studio\2017\Community\Licenses\Windows 8.1 SDK
License.rtf
   - \Program Files (x86)\Microsoft Visual Studio\2017\Community\Licenses\Windows 8 SDK Third
Party Notices.rtf
   - \Program Files (x86)\Microsoft Visual Studio\2017\Community\Licenses\Windows 8 SDK
License.rtf
   - \Program Files (x86)\Microsoft Visual Studio\2017\Community\Licenses\1046\NuGetEula.rtf
   - \Program Files (x86)\Microsoft Visual Studio\2017\Community\Licenses\1045\NuGetEula.rtf
   - \Program Files (x86)\Microsoft Visual Studio\2017\Community\Licenses\1042\NuGetEula.rtf
   - \Program Files (x86)\Microsoft Visual Studio\2017\Community\Licenses\1041\NuGetEula.rtf
   - \Program Files [...]
```

93962 - Microsoft Security Rollup Enumeration

Synopsis

This plugin enumerates installed Microsoft security rollups.

Description

Nessus was able to enumerate the Microsoft security rollups installed on the remote Windows host.

See Also

http://www.nessus.org/u?b23205aa

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/10/11, Modification date: 2020/06/10

Ports

vda-it-ts (TCP/445) Vulnerability State: Resurfaced

```
Cumulative Rollup : 06_2020 [KB4560960]

Latest effective update level : 06_2020
File checked                  : C:\WINDOWS\system32\ntoskrnl.exe
File version                  : 10.0.18362.900
Associated KB                 : 4560960
```

51351 - Microsoft .NET Framework Detection

Synopsis

A software framework is installed on the remote host.

Description

Microsoft .NET Framework, a software framework for Microsoft Windows operating systems, is installed on the remote host.

See Also

https://www.microsoft.com/net

http://www.nessus.org/u?15ae6806

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/12/20, Modification date: 2020/05/29

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Nessus detected 5 installs of Microsoft .NET Framework:

  Path         : C:\Windows\Microsoft.NET\Framework64\v2.0.50727
  Version      : 2.0.50727
  Full Version : 2.0.50727.4927
  SP           : 2

  Path         : C:\Windows\Microsoft.NET\Framework64\v3.0
  Version      : 3.0
  Full Version : 3.0.30729.4926
  SP           : 2

  Path         : C:\Windows\Microsoft.NET\Framework64\v3.5\
  Version      : 3.5
  Full Version : 3.5.30729.4926
  SP           : 1

  Path         : C:\Windows\Microsoft.NET\Framework64\v4.0.30319\
  Version      : 4.8
  Full Version : 4.8.03752
  Install Type : Full

  Path         : C:\Windows\Microsoft.NET\Framework64\v4.0.30319\
  Version      : 4.8
  Full Version : 4.8.03752
  Install Type : Client
```

11457 - Microsoft Windows SMB Registry : Winlogon Cached Password Weakness

Synopsis

User credentials are stored in memory.

Description

The registry key 'HKLM\Software\Microsoft\WindowsNT\CurrentVersion\ Winlogon\CachedLogonsCount' is not 0.
Using a value greater than 0 for the CachedLogonsCount key indicates that the remote Windows host locally caches the passwords of the users when they login, in order to continue to allow the users to login in the case of the failure of the primary domain controller (PDC).
Cached logon credentials could be accessed by an attacker and subjected to brute force attacks.

See Also

http://www.nessus.org/u?184d3eab

http://www.nessus.org/u?fe16cea8

https://technet.microsoft.com/en-us/library/cc957390.aspx

Solution

Consult Microsoft documentation and best practices.

Risk Factor

None

Plugin Information:

Publication date: 2003/03/24, Modification date: 2018/06/05

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
  Max cached logons : 10
```

10859 - Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration

Synopsis

It is possible to obtain the host SID for the remote host.

Description

By emulating the call to LsaQueryInformationPolicy(), it was possible to obtain the host SID (Security Identifier).
The host SID can then be used to get the list of local users.

See Also

http://technet.microsoft.com/en-us/library/bb418944.aspx

Solution

You can prevent anonymous lookups of the host SID by setting the 'RestrictAnonymous' registry setting to an appropriate value.
Refer to the 'See also' section for guidance.

Risk Factor

None

Plugin Information:

Publication date: 2002/02/13, Modification date: 2019/10/04

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
The remote host SID value is :

1-5-21-330363374-4240072399-3876068862

The value of 'RestrictAnonymous' setting is : 0
```

92364 - Microsoft Windows Environment Variables

Synopsis

Nessus was able to collect and report environment variables from the remote host.

Description

Nessus was able to collect system and active account environment variables on the remote Windows host and generate a report as a CSV attachment.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2020/01/22

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
Environment variable information attached.
```

92366 - Microsoft Windows Last Boot Time

Synopsis

Nessus was able to collect the remote host's last boot time in a human readable format.

Description

Nessus was able to collect and report the remote host's last boot time as an ISO 8601 timestamp.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2018/07/09

Ports

vda-it-ts (TCP/0) Vulnerability State: Active

```
Last reboot : 2020-06-16T20:36:36+01:00 (20200616203636.500000+060)
```

122778 - Security Update for .NET Core SDK (March 2019)

Synopsis

The remote Windows host is affected by a tampering vulnerability.

Description

The remote Windows host has an installation of .NET Core SDK with a version of 1.x < 1.1.13 or 2.1.x < 2.1.505. Therefore, the host is affected by a tampering vulnerability with in the NuGet Package Manager. An authenticated, attacker can exploit this, via manipulating the folder contents prior to building or installing a application, to modify files and folders after unpacking.

See Also

https://github.com/dotnet/announcements/issues/103

http://www.nessus.org/u?8b5a86c1

http://www.nessus.org/u?0225f3cc

http://www.nessus.org/u?7c0a5e95

Solution

Refer to vendor documentation.

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

3.6

CVSS v3.0 Base Score

6.5 (AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N)

CVSS v3.0 Temporal Score

5.7 (E:U/RL:O/RC:C)

CVSS Base Score

4.0 (AV:N/AC:L/Au:S/C:N/I:P/A:N)

CVSS Temporal Score

3.0 (E:U/RL:OF/RC:C)

References

CVE	CVE-2019-0757

Plugin Information:

Publication date: 2019/03/12, Modification date: 2020/01/17

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Path              : C:\\program files\dotnet\\sdk\2.1.402
Installed version : 2.1.402.0
Fixed version     : 2.1.505
```

33545 - Oracle Java Runtime Environment (JRE) Detection

Synopsis

There is a Java runtime environment installed on the remote Windows host.

Description

One or more instances of Oracle's (formerly Sun's) Java Runtime Environment (JRE) is installed on the remote host. This may include private JREs bundled with the Java Development Kit (JDK).
- Additional instances of Java may be discovered if thorough tests are enabled.

See Also

https://www.oracle.com/technetwork/java/index.html

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2008/07/18, Modification date: 2019/12/09

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
Nessus detected 13 installs of Java Runtime:

  Path    : C:\Program Files\Java\jdk1.8.0_181\jre
  Version : 1.8.0_181

  Path    : C:\Program Files (x86)\Java\jdk1.8.0_181\jre
  Version : 1.8.0_181

  Path    : C:\Documents and Settings\All Users\Oracle\Java\javapath\java.exe
  Version : 1.8.0_171

  Path    : C:\Documents and Settings\All Users\Oracle\Java\javapath_target_529031\java.exe
  Version : 1.8.0_171

  Path    : C:\Program Files (x86)\Java\jdk1.8.0_181\bin\java.exe
  Version : 1.8.0_181

  Path    : C:\Program Files (x86)\Java\jdk1.8.0_181\jre\bin\java.exe
  Version : 1.8.0_181

  Path    : C:\Program Files\DBeaver\jre\bin\java.exe
  Version : 1.8.0_77

  Path    : C:\Program Files\Java\jdk1.8.0_181\bin\java.exe
  Version : 1.8.0_181

  Path    : C:\Program Files\Java\jdk1.8.0_181\jre\bin\java.exe
  Version : 1.8.0_181

  Path    : C:\ProgramData\Oracle\Java\javapath\java.exe
  Version : 1.8.0_171

  Path    : C:\ProgramData\Oracle\Java\javapath_target_529031\java.exe
  Version : 1.8.0_171

  Path    : C:\Users\All Users\Oracle\Java\javapath\java.exe
  Version : 1.8.0_171

  Path    : C:\Users\All Users\Oracle\Java\javapath_target_529031\java.exe
  Version : 1.8.0_171
```

66424 - Microsoft Malicious Software Removal Tool Installed

Synopsis

An antimalware application is installed on the remote Windows host.

Description

The Microsoft Malicious Software Removal Tool is installed on the remote host. This tool is an application that attempts to detect and remove known malware from Windows systems.

See Also

http://www.nessus.org/u?47a3e94d

https://support.microsoft.com/en-us/help/891716

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/05/15, Modification date: 2020/04/22

Ports

vda-it-ts (TCP/445) Vulnerability State: Active

```
File                : C:\WINDOWS\system32\MRT.exe
Version             : 5.82.17046.2
Release at last run : unknown
Report infection information to Microsoft : Yes
```